明 細 書

認証システム

技術分野

[0001] 本発明は、通信相手の正当性を認証する技術に関する。

背景技術

[0002] 近年、インターネットの利用の急速な広がりにより、インターネットを通信の基盤とするシステムが増加している。例えば、インターネットを介して物品の売買を行う電子商取引もその1つである。

このような、インターネットを通信の基盤とするシステムにおいては、通信相手がシステムの正当な参加者であることを確認することが必須となる。これを認証という。通信相手としては人間が機器を操作している場合や、機器が予め決められた手順で処理を行う場合があるが、以下ではこの両者を含めて機器と呼ぶこととする。また、通信相手を認証することを機器認証という。なお、機器自身の正当性を示すこと、すなわち自分がシステムの正当な参加者であることを示すことを「証明する」といい、相手の正当性を確認することを「検証する」という。認証とは、証明と検証の両方を含む概念である。

[0003] また、上述した通信のシステムにおいては、情報の秘密通信、前記認証などのために暗号技術が用いられる。暗号技術には共通鍵暗号方式と公開鍵暗号方式とがある。共通鍵暗号方式では、暗号化のための鍵と復号のための鍵が同一である。一方、公開鍵暗号方式では、暗号化のための鍵と復号のための鍵が異なる。

前記認証を行うには公開鍵暗号方式を用いる方が望ましい。なぜならば、共通鍵暗号方式を用いた認証、いわゆるパスワード方式においては，検証者は証明者と同じ秘密を持つので、最初の認証以降、検証者が証明者になりすます危険性がある。一方、公開鍵暗号方式を用いた認証においては，証明者は公開鍵暗号の秘密鍵を用いて証明し、検証者はその秘密鍵に対する公開鍵を用いて検証する。公開鍵暗号方式では、公開鍵から秘密鍵を作成できないようになっているので、認証が終わった後で、検証者が証明者になりすますことができない。

[0004] なお、公開鍵暗号方式において、秘密鍵を用いて、正当性を確認するためのデータ(署名文又は署名データと呼ぶ)を生成することを署名といい、秘密鍵に対応する公開鍵を用いて、その署名データの正当性を確認することを署名検証という。

公開鍵暗号方式を用いた相手認証処理の例として、第1の機器が第2の機器にチャレンジデータとして乱数データを送信し、続いて、第2の機器がその乱数データに対して自分の秘密鍵で署名を行って第1の機器にレスポンスデータを返信し、最後に、返信されてきた署名文に対して、第1の機器が第2の機器の公開鍵を用いて検証するというものがある。一般に、このような公開鍵暗号を用いた認証においては、公開鍵そのものが当該システム内で有効なものであることが前提となる。

[0005] このために、当該システムにおいて認証局(Certification Authority:以下、CA)と呼ばれる機関から、各機器に対応する公開鍵が正しいことを示す、つまり、公開鍵に対する「お墨付き」となる「公開鍵証明書」が発行されることが一般的である。CAは、機器の識別名、有効期限及び公開鍵などを結合したデータに対して、CAの電子署名データを生成し、この結合データと生成した電子署名データとから構成される公開鍵証明書を生成し、生成した公開鍵証明書を配布する。公開鍵証明書を受け取った機器は、そのデータに対する認証局の電子署名データの正しさを確認し、さらに相手機器の識別名や現在の時間からその公開鍵証明書の記載内容を確認した上で、公開鍵の正しさを確認する。さらに、発行された公開鍵証明書のうち、システムから排除され, 正当ではないとされる機器の公開鍵証明書については、それらが無効化されていることを他の機器に知らせるために、無効化した公開鍵証明書を特定する情報の一覧に対して認証局の電子署名データが付与された公開鍵証明書無効化リスト(Certificate Revocation List:以下、CRL)が発行される。

[0006] このように、相手機器の公開鍵を用いてその相手機器を認証する際には、その相手機器の公開鍵証明書を入手し、入手した公開鍵証明書がCRLに登録されたもの(無効化されたもの)でないことを確認した上で、上述の認証処理を行うことで、不正な相手機器との取引を回避することができる。CRLの形式、実現例等は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。なお、ISO/IEC/ITUが定めたX. 509標準において、CRL形式、つまりCRLのデータ構造が

定義されている。

[0007] 無効化された公開鍵証明書が増えると、その都度、無効化された公開鍵証明書の識別子を追加する更新がCRLに対してなされ、更新された新たなCRLが各端末装置に配布される。

発明の開示

発明が解決しようとする課題

[0008] しかしながら、新たなCRLが各端末装置に配布されたとしても、各端末装置が、新たなCRLにより自身が保持している古いCRLを更新するとは限らない。なぜなら、当該端末装置にとっては、CRLの更新による直接のメリットがないからである。例えば、古いCRLを用いることにより、無効化される前の公開鍵証明書に対応する端末装置、つまり現時点では無効化された端末装置との通信が可能である。このため、無効化された端末装置の利用を停止することが困難であるという問題点がある。

[0009] 本発明は、上記の問題点を解決し、対象物が無効か否かを示すブラックリストを強制的に更新することができる認証システム、判定装置、判定方法及び判定用のコンピュータプログラムを提供することを目的とする。

課題を解決するための手段

[0010] 上記目的を達成するために、本発明は、ブラックリストを用いて対象物が無効か否かを判定する判定装置であって、対象物が無効か否かを示すブラックリスト及び自身が有効か否かを示すホワイトリストを保持する保持手段と、前記ホワイトリストを更新するか否かを判定する判定手段と、更新すると判定される場合に、最新のブラックリスト及び最新のホワイトリストを同時に取得する取得手段と、取得した最新のブラックリスト及び最新のホワイトリストを前記保持手段に同時に上書きする更新手段とを備えることを特徴とする。

発明の効果

[0011] ホワイトリストは、装置自身の有効性を示すので、ホワイトリストの更新は、自身にメリットがある。例えば、ホワイトリストが最新に更新がされないと、通信相手から通信が拒否される場合がある。

この構成によると、上記のような性質を有するホワイトリストを更新すると判定する場合に、同時にブラックリストも更新するので、ブラックリストの更新を強制することができる。

[0012] ここで、前記対象物は、情報を記録するために用いられる記録媒体であり、前記保持手段は、前記ブラックリストとして、前記記録媒体が無効か否かを示す媒体ブラックリストを保持しており、前記取得手段は、前記最新のブラックリストとして、前記記録媒体が無効か否かを示す最新の媒体ブラックリストを取得し、前記更新手段は、取得した前記媒体ブラックリストを前記保持手段に上書きするとしてもよい。

[0013] この構成によると、記録媒体を対象物とすることができる。

ここで、前記対象物は、デジタル著作物であり、前記保持手段は、前記ブラックリストとして、前記デジタル著作物が無効か否かを示す著作物ブラックリストを保持しており、前記取得手段は、前記最新のブラックリストとして、前記デジタル著作物が無効か否かを示す最新の著作物ブラックリストを取得し、前記更新手段は、取得した前記著作物ブラックリストを前記保持手段に上書きするとしてもよい。

[0014] この構成によると、デジタル著作物を対象物とすることができる。

ここで、

前記対象物は、情報取得装置であり、前記保持手段は、前記ブラックリストとして、前記情報取得装置が無効か否かを示す装置ブラックリストを保持しており、前記取得手段は、前記最新のブラックリストとして、前記情報取得装置が無効か否かを示す最新の装置ブラックリストを取得し、前記更新手段は、取得した前記装置ブラックリストを前記保持手段に上書きするとしてもよい。

[0015] この構成によると、情報取得装置を対象物とすることができる。

ここで、前記情報取得装置は、情報を記録するために用いられる記録媒体に対して情報を書き込み又は前記記録媒体から情報を読み出す媒体アクセス装置であるとしてもよい。

この構成によると、媒体アクセス装置を対象物とすることができる。

ここで、前記情報取得装置は、デジタル放送により放送される情報を受信するデジタル放送受信装置であるとしてもよい。

[0016] この構成によると、デジタル放送受信装置を対象物とすることができる。

ここで、前記判定手段は、前記ホワイトリストの世代を示す世代情報を用いて、更新の判定を行うとしてもよい。

この構成によると、各ホワイトリストの新旧の判定を確実に行うことができる。

図面の簡単な説明

[0017] [図1]本発明に係る認証システム10の全体構成を示す構成図である。

[図2]記録媒体300に記録されているデータ構造の一例を示すデータ構造図である。

[図3]リストDのデータ構造の一例を示すデータ構造図である。

[図4]リストHのデータ構造の一例を示すデータ構造図である。

[図5]ドライブ装置100及びパーソナルコンピュータ200の構成を示すブロック図である。

[図6]認証システム10の主要な動作を示すフローチャートである。図7へ続く。

[図7]認証システム10の主要な動作を示すフローチャートである。図8へ続く。

[図8]認証システム10の主要な動作を示すフローチャートである。図9へ続く。

[図9]認証システム10の主要な動作を示すフローチャートである。図8から続く。

[図10]ドライブ装置100とパーソナルコンピュータ200との間で設定されるSACの実現の動作を示すフローチャートである。

[図11]認証システム10bのパーソナルコンピュータ200bの構成を示すブロック図である。

[図12]証明書識別子リスト600のデータ構造の一例を示すデータ構造図である。

[図13]証明書識別子リスト700のデータ構造の一例を示すデータ構造図である。

[図14]証明書識別子リスト800のデータ構造の一例を示すデータ構造図である。

符号の説明

[0018] 10 認証システム

10b 認証システム

20 インターネット

30 認証局装置

30b 認証局装置
40 通信路
100 ドライブ装置
100 パーソナルコンピュータ
101 入出力部
102 入出力部
103 公開鍵格納部
104 検証部
105 証明書格納部
106 証明書送信部
107 公開鍵暗号処理部
108 暗号化部
200 パーソナルコンピュータ
200b パーソナルコンピュータ
201 入出力部
202 比較更新部
202b 比較更新部
203 通信部
204 デバイス鍵格納部
205 復号部
206 最新リスト格納部
206b 最新リスト格納部
207 証明書格納部
208 最新リスト格納部
208 証明書送信部
208b 証明書送信部
209 最新リスト格納部
210 検証部

210b 検証部

211 公開鍵格納部

212 パーソナルコンピュータ

212 公開鍵暗号処理部

213 復号部

214 復号部

215 復号部

216 再生部

217 モニタ

218 スピーカ

221 制御部

230 システムLSI

230b システムLSI

300 記録媒体

発明を実施するための最良の形態

[0019] 1. 第1の実施の形態

本願の発明の1の実施の形態としての認証システム10について説明する。

1. 1 認証システム10の構成

認証システム10は、図1に示すように、ドライブ装置100、パーソナルコンピュータ200及び認証局装置30から構成されている。

[0020] パーソナルコンピュータ200は、インターネット20を介して、認証局装置30に接続されている。

また、ドライブ装置100とパーソナルコンピュータ200とは、汎用の通信路40を介して接続されている。ここで、汎用の通信路とは、その仕様が公開されているため、通信路上のデータ盗聴、改ざん、差し替えなどの危険に晒される安全でない通信路のことである。

[0021] 認証局装置30は、公開鍵の正当性を示す公開鍵証明書と、ドライブ装置100が保持する公開鍵証明書の有効性を示すリスト(以下、リストD)と、パーソナルコンピュー

タ200が保持する公開鍵証明書の有効性を示すリスト(以下、リストH)を発行し、パーソナルコンピュータ200は、予め、リストD及びリストHを保持している。

ドライブ装置100には、暗号化されたコンテンツ(以下、暗号化コンテンツと呼ぶ。)を記録している記録媒体300が装着されている。

[0022] パーソナルコンピュータ200は、自身が保持しているリストDを検索して、通信相手であるドライブ装置100が保持する公開鍵証明書が有効か否かを判断する。さらに、パーソナルコンピュータ200は、自身が保持しているリストHを検索して、通信相手であるドライブ装置100に対して、自身が保持する公開鍵証明書が有効であることを示すリストHの部分データを送信する。ドライブ装置100は、パーソナルコンピュータ200から送られるリストHの部分データのみを検証/確認する。こうして、パーソナルコンピュータ200の有効性を判断することが可能となるため、ドライブ装置100の処理負荷を軽減することができる。

[0023] さらに、パーソナルコンピュータ200は、自身の保持する公開鍵証明書の有効性を示すリストHの更新が必要な場合、インターネット20を介して認証局装置30に接続し、認証局装置30から更新版のリストHを取得する。その時、更新版のリストDも同様に取得する。

次に、ドライブ装置100及びパーソナルコンピュータ200の一方が他方を認証する片方向認証、又は両者が互いに認証し合う相互認証を実施した後、認証が成功すれば、ドライブ装置100は、記録媒体300から暗号化コンテンツを読み出し、読み出した暗号化コンテンツをパーソナルコンピュータ200へ送信する。パーソナルコンピュータ200は、ドライブ装置100から暗号化コンテンツを受け取り、受け取った暗号化コンテンツを復号して、復号コンテンツを生成し、生成した復号コンテンツを再生する。

[0024] 1.2 記録媒体300の構成

記録媒体300は、一例として、ビデオやオーディオ、コンピュータのデータなどを記録するための大容量の光ディスクメディアであるDVD(Digital Versatile Disc)である。

記録媒体300は、図2に示すように、バージョン番号記録領域311、暗号化メディア鍵記録領域312、暗号化コンテンツ鍵記録領域313及び暗号化コンテンツ記録領域

314を備えており、バージョン番号記録領域311には、バージョン番号MVN301が記録され、暗号化メディア鍵記録領域312には、暗号化メディア鍵群302が記録され、暗号化コンテンツ鍵記録領域313には、暗号化コンテンツ鍵303が記録され、暗号化コンテンツ記録領域314には、暗号化コンテンツ304が記録されている。

[0025] バージョン番号MVN301は、記録媒体300に記録されているデータを利用する際に適用されるべきリストD及びリストHの世代を示す番号である。図2において、バージョン番号MVN301は、一例として、「0003」である。バージョン番号は、数値で示され、数値が大きいほど、新しい世代であることを示している。本明細書において、他のバージョン番号についても同様である。

[0026] 暗号化メディア鍵群302は、ある特定の装置にだけメディア鍵を与えるために構成されたデータであり、メディア鍵を与える装置が持つデバイス鍵(DK)を用いて、メディア鍵Kmを暗号化し、また、メディア鍵を与えない装置が持つデバイス鍵DKを用いて、メディア鍵とは全く無関係なダミーデータを暗号化して構成されている。

暗号化メディア鍵群302は、n個の暗号化メディア鍵から構成されている。ここで、nは、認証システム10に属している装置の総数を示しており、n個の暗号化メディア鍵は、n台の装置に対応している。各暗号化メディア鍵は、当該暗号化メディアに対応する装置のデバイス鍵DKi を用いて、メディア鍵Km又はメディア鍵とは全く無関係なダミーデータに、暗号化アルゴリズムEを施して生成されたものである。メディア鍵Kmは、記録媒体300に記録されているデータに固有の鍵情報である。ここで、例えば、第1の装置のデバイス鍵DK1を用いて生成された暗号化メディア鍵をE(DK1、Km)と表現している。なお、この明細書において、E(A、B)は、鍵Aを用いて、平文Bに暗号化アルゴリズムEを施して生成された暗号文を示している。

[0027] 図2においては、暗号化メディア鍵群302には、暗号化メディア鍵E(DK3、0)及び(DK10、0)が含まれている。これらの暗号化メディア鍵は、デバイス鍵「DK3」を持つ装置と、デバイス鍵「DK10」を持つ装置に対してはメディア鍵を与えない場合の例を示している。

暗号化コンテンツ鍵303は、メディア鍵Kmを用いて、コンテンツ鍵Kcに暗号化アルゴリズムEを施して生成されたものである。

[0028] 暗号化コンテンツ鍵＝E(Km、Kc)

暗号化コンテンツ304は、コンテンツ鍵Kcを用いて、コンテンツCに暗号化アルゴリズムEを施して生成されたものである。

ここで、暗号化アルゴリズムEは、一例として、共通鍵暗号方式のDES(Data Encryption Standard)によるものである。

[0029] 1．3 リストD及びリストHの構成

ドライブ装置100の有効性を判断するためのリストDの構成、及びパーソナルコンピュータ200の有効性を判断するためのリストHの構成の一例について説明する。

(1)リストDの構成

図3に示すリストD400は、ドライブ装置100が保持する公開鍵証明書のうち、識別子DID＝1、DID＝6、DID＝7、DID＝15により識別される4つの公開鍵証明書が無効化され、他の識別子により識別される他の公開鍵証明書が無効化されていない場合の例を示している。また、この図の参照符号410により示される枠内に、各識別子を表示しており、×印が付された番号は、無効化された公開鍵証明書の識別子を示している。×印が付されていない番号は、無効化されていない公開鍵証明書の識別子を示している。

[0030] リストD400は、図3に示すように、バージョン番号フィールド401、識別子数フィールド402、無効化識別子フィールド403及び署名フィールド403から構成されている。バージョン番号フィールド401には、バージョン番号DVN401aが格納されており、識別子数フィールド402には、識別子数402aが格納されており、無効化識別子フィールド403には、4個の無効化識別子DID_1 411、DID_2 412、DID_3 413、DID_4 414が格納されており、署名フィールド403には、CAの署名データ404aが格納されている。

[0031] ここで、バージョン番号DVN401aは、リストD400の世代を示す番号であり、図3に示す例では、「0003」である。

識別子数402aは、無効化識別子フィールド403に格納されている無効化識別子の数を示しており、図3に示す例では、「0004」である。

無効化識別子DID_1 411、DID_2 412、DID_3 413、DID_4 414は、無効化すべき公

開鍵証明書の識別番号を示し、図3に示す例では、「0001」、「0006」、「0007」、「0015」である。

[0032] CAの署名データ404aは、CAにより生成され、前記フィールドの正当性を検証するための署名データであり、CAの秘密鍵SK__CAを用いて、バージョン番号401aと4個の無効化識別子DID_1 411、DID_2 412、DID_3 413、DID_4 414とをこの順序で、連結して生成される連結データに、デジタル署名アルゴリズムSigを施して生成されたものである。

[0033] CAの署名データ

$$=Sig(SK\_\_CA, DVN||DID_1||DID_2||DID_3||DID_4)$$

また、記号「||」は、前後のデータを連結することを意味する記号として用い、関数Sig(X, Y)は、鍵データXを用いて、データYに対してデジタル署名SiGを施して、署名生成を行う関数として用いる。また、SK__CAはCAだけが保持する署名生成に利用する秘密鍵のことである。

[0034] CAの署名データは、リストD400に含まれる各フィールドの各データが正しいことを証明するために用いられる。

このように、リストD400は、無効化されている公開鍵証明書の識別子を含んでいるので、リストD400をブラックリストと呼ぶこともある。

なお、CAの署名データは、リストD400に含まれるデータのうち、CAの署名データ及び識別子数を除く他のデータに対して生成された署名データであるが、CAの署名データを除く他の全てのデータに対して生成された署名データであるとしてもよい。

[0035] また、前記署名データは、必ずしもデータの連結値そのものから生成される必要はなく、データの連結値のハッシュ値から署名データを生成する形態であってもよい。さらに、前記署名は、付録型の署名である必要はなく、署名検証実施後、署名対象データが生成される回復型の署名であってもよい。この場合、リストDには無効化識別子フィールドが含まれておらず、検証時に署名データから無効化識別子が生成される。

[0036] (2)リストHの構成

図4に示すリストH500は、パーソナルコンピュータ200が保持する公開鍵証明書のうち、識別子HID＝1、HID＝5、HID＝9、HID＝13ー16により識別子される7つの公開鍵証明書が無効化され、他の識別子により識別される他の公開鍵証明書が無効化されていない場合の例を示している。また、この図の参照符号520により示される枠内に、各識別子を表示しており、×印が付された番号は、無効化された公開鍵証明書の識別子を示している。×印が付されていない番号は、無効化されていない公開鍵証明書の識別子を示している。

[0037] 枠520において、×印が付されていない番号の最初の区間521は、識別子の集合{2、3、4}から構成され、×印が付されていない番号の次の区間522は、識別子の集合{6、7、8}から構成され、×印が付されていない番号の次の区間523は、識別子の集合{10、11、12}から構成され、×印が付されていない番号の次の区間524は、識別子の集合{17、18、・・・、9999}から構成されている。

[0038] リストH500は、図4に示すように、バージョン番号フィールド501、組数フィールド502、有効識別子フィールド511及び署名フィールド512から構成されている。バージョン番号フィールド501には、バージョン番号HVN501aが格納されており、組数フィールド502には、組数502aが格納されており、有効識別子フィールド511には、8個の識別子503a、503b、504a、504b、505a、505b、506a、506bが格納されており、署名フィールド512には、4個の署名データ507ー510が格納されている。

[0039] ここで、バージョン番号HVN501aは、リストH500の世代を示す番号であり、図4に示す例では、「0003」である。

組数502aは、有効な公開鍵証明書の識別子が連続する区間の数を示しており、図4に示す例では、「0004」であり、区間が4個存在することを示している。

2個の識別子503a、503bは、組503を構成し、2個の識別子504a、504bは、組504を構成し、2個の識別子505a、505bは、組505を構成し、2個の識別子506a、506bは、組506を構成している。各組は、有効な公開鍵証明書の識別子が連続する区間の先頭の識別子と最後の識別子から構成される。

[0040] 図4に示す例では、組503は、識別子「0002」を先頭とし、識別子「0004」を最後とする区間521を示しており、組504は、識別子「0006」を先頭とし、識別子「0008」を

最後とする区間522を示しており、組505は、識別子「0010」を先頭とし、識別子「0012」を最後とする区間523を示しており、組506は、識別子「0017」を先頭とし、識別子「9999」を最後とする区間524を示している。

[0041] 署名フィールド512には、4個の署名データ507ー510が格納されており、署名データ507は、組503に対応し、署名データ508は、組504に対応し、署名データ509は、組505に対応し、署名データ510は、組506に対応している。

4個の署名データ507ー510は、それぞれ、CAにより生成され、リストH500に含まれ、対応する各組のデータの正当性を検証するための署名データである。

[0042] 署名データ507は、CAの秘密鍵SK_CAを用いて、バージョン番号HVN501aと、組503に含まれている識別子HID_1 503aと、識別子HID_2 503bとをこの順序で、連結して生成される連結データに、デジタル署名アルゴリズムSigを施して生成されたものである。

CAの署名データ

$=Sig(SK\_CA, HVN||HID_1||HID_2)$

署名データ508は、CAの秘密鍵SK_CAを用いて、バージョン番号HVN501aと、組504に含まれている識別子HID_3 504aと、識別子HID_4 504bとをこの順序で、連結して生成される連結データに、デジタル署名アルゴリズムSigを施して生成されたものである。

[0043] CAの署名データ

$=Sig(SK\_CA, HVN||HID_3||HID_4)$

署名データ509は、CAの秘密鍵SK_CAを用いて、バージョン番号HVN501aと、組505に含まれている識別子HID_5 505aと、識別子HID_6 505bとをこの順序で、連結して生成される連結データに、デジタル署名アルゴリズムSigを施して生成されたものである。

[0044] CAの署名データ

$=Sig(SK\_CA, HVN||HID_5||HID_6)$

署名データ510は、CAの秘密鍵SK_CAを用いて、バージョン番号HVN501aと、組506に含まれている識別子HID_7 506aと、識別子HID_8 506bとをこの順序で、

連結して生成される連結データに、デジタル署名アルゴリズムSigを施して生成されたものである。

[0045] CAの署名データ

$=Sig(SK\_\_CA, HVN||HID_7||HID_8)$

このように、リストH500は、無効化されていない公開鍵証明書の識別子を含んでいるので、リストH500をホワイトリストと呼ぶこともある。

CAの署名データは、リストH500に含まれる各有効識別子フィールドの区間のデータが正しいことを証明するために用いられる。

[0046] なお、前記署名データは、必ずしも複数のデータの連結値から生成される必要はなく、複数のデータの連結値のハッシュ値から生成される形態であってもよい。さらに、前記署名は、付録型の署名である必要はなく、署名検証実施後、署名対象データが生成される回復型の署名であってもよい。この場合、リストHには有効識別子フィールドが含まれておらず、検証時に署名データから有効区間の先頭の識別子及び終端の識別子が生成される。

[0047] 1．4 ドライブ装置100の構成

ドライブ装置100は、図5に示すように、入出力部101、入出力部102、公開鍵格納部103、検証部104、証明書格納部105、証明書送信部106、公開鍵暗号処理部107及び暗号化部108から構成されている。

(1)入出力部101及び入出力部102

入出力部101は、ドライブ装置100の他の構成要素による指示により、記録媒体300から情報を読み出し、当該他の構成要素に対して、読み出した情報を出力する。

[0048] 入出力部102は、ドライブ装置100の他の構成要素による指示により、当該他の構成要素から情報を受け取り、受け取った情報をパーソナルコンピュータ200へ出力する。また、パーソナルコンピュータ200から情報を受け取り、受け取った情報を、パーソナルコンピュータ200の指示により、ドライブ装置100の他の構成要素へ出力する。

(2)公開鍵格納部103及び証明書格納部105

公開鍵格納部103は、予め、CAの公開鍵PK__CAを格納している。ドライブ装置

100の製造業者は、CAからCAの公開鍵PK_CAを入手し、ドライブ装置100が製造される際に、製造業者によりCAの公開鍵PK_CAが公開鍵格納部103へ書き込まれる。

[0049] 証明書格納部105は、予め、ドライブ装置100の公開鍵証明書を格納している。ドライブ装置100の製造業者は、CAからドライブ装置100の公開鍵証明書を入手し、ドライブ装置100が製造される際に、製造業者によりドライブ装置100の公開鍵証明書が証明書格納部105へ書き込まれる。

ドライブ装置100の公開鍵証明書は、CAにより生成されたものであり、ドライブ装置100の公開鍵、当該公開鍵を識別する識別子、当該公開鍵の正当性を証明するためのCAの署名データなどを含んで構成されている。

[0050] (3)検証部104

検証部104は、パーソナルコンピュータ200から入出力部102を介して、部分リスト及び公開鍵証明書を受け取り、公開鍵格納部103からCAの公開鍵PK_CAを読み出し、読み出した公開鍵PK_CAを用いて、受け取った部分リストに含まれる署名データに対して署名検証を施す。署名検証に失敗すると、以降の処理を中止する。署名検証に成功すると、さらに、読み出した公開鍵PK_CAを用いて、受け取った公開鍵証明書に含まれる署名データに対して署名検証を施す。署名検証に失敗すると、以降の処理を中止する。

[0051] 署名検証に成功すると、さらに、検証部104は、部分リストと公開鍵証明書とを用いて、当該公開鍵証明書が有効か否かを検証する。具体的には、検証部104は、受け取った前記公開鍵証明書に含まれる識別子が、前記部分リストに含まれているか否かを判断する。識別子が部分リストに含まれている場合には、前記公開鍵証明書は有効であると判断し、識別子が部分リストに含まれていない場合には、前記公開鍵証明書は無効であると判断する。無効であると判断する場合には、以降の処理を中止する。有効であると判断する場合には、認証の成功を示す検証成功情報を公開鍵暗号処理部107へ出力する。

[0052] (4)証明書送信部106

証明書送信部106は、証明書格納部105からドライブ装置100の公開鍵証明書を

読み出し、読み出した公開鍵証明書を入出力部102を介して、パーソナルコンピュータ200へ出力する。

(5)公開鍵暗号処理部107

公開鍵暗号処理部107は、ドライブ装置100とパーソナルコンピュータ200と接続する汎用の通信路40上で情報を安全に送信するための認証付き通信路(Secure Authentication Channel:SAC)を確立するのに必要な認証／鍵共有処理を実行する。前記鍵共有処理において、パーソナルコンピュータ200と共有するセッション鍵を生成する。

[0053] (6)暗号化部108

暗号化部108は、入出力部101を介して、記録媒体300から暗号化コンテンツ鍵303を読み出し、公開鍵暗号処理部405により生成されたセッション鍵を用いて、読み出した暗号コンテンツ鍵に暗号化アルゴリズムを施して、二重暗号化コンテンツ鍵を生成し、生成した二重暗号化コンテンツ鍵を、入出力部102を介して、パーソナルコンピュータ200へ出力する。

[0054] 1.5 パーソナルコンピュータ200

パーソナルコンピュータ200は、図5に示すように、入出力部201、システムLSI(大規模集積回路、Large Scale Integrated circuit)230、通信部203、再生部216、制御部221及び図示していない他の構成要素から構成される。

なお、パーソナルコンピュータ200は、具体的には、前記システムLSI、マイクロプロセッサ、ROM、RAM、バス、ハードディスクユニット、通信ユニットなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、パーソナルコンピュータ200は、その一部の機能を達成する。

[0055] システムLSI230は、図5に示すように、比較更新部202、最新リスト格納部206、証明書格納部207、証明書送信部208、最新リスト格納部209、検証部210、公開鍵格納部211、公開鍵暗号処理部212、復号部213、復号部214及び復号部215から構成されている。

システムLSI230は、上記の複数の構成部を1個のチップ上に集積して製造された超多機能LSIであり、具体的には、マイクロプロセッサ、ROM、RAMなどを含んで構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、システムLSI230は、その一部の機能を達成する。

[0056] (1)証明書格納部207、最新リスト格納部206、最新リスト格納部209、公開鍵格納部211及びデバイス鍵格納部204

証明書格納部207は、予め、パーソナルコンピュータ200の公開鍵証明書を格納している。パーソナルコンピュータ200の製造業者は、CAからパーソナルコンピュータ200の公開鍵証明書を入手し、パーソナルコンピュータ200が製造される際に、製造業者によりパーソナルコンピュータ200の公開鍵証明書が証明書格納部207へ書き込まれる。

[0057] パーソナルコンピュータ200の公開鍵証明書は、CAにより生成されたものであり、パーソナルコンピュータ200の公開鍵、当該公開鍵を識別する識別子、当該公開鍵の正当性を証明するためのCAの署名データなどを含んで構成されている。

最新リスト格納部206は、予め、パーソナルコンピュータ200の公開鍵証明書の有効性を示すリストHを格納している。リストHについては、上述した通りである。パーソナルコンピュータ200の製造業者は、CAからリストHを入手し、パーソナルコンピュータ200が製造される際に、製造業者によりリストHが最新リスト格納部206へ書き込まれる。

[0058] 最新リスト格納部209は、予め、ドライブ装置100の公開鍵証明書の有効性を示すリストDを格納している。リストDについては、上述した通りである。パーソナルコンピュータ200の製造業者は、CAからリストDを入手し、パーソナルコンピュータ200が製造される際に、製造業者によりリストDが最新リスト格納部209へ書き込まれる。

公開鍵格納部211は、予め、CAの公開鍵PK_CAを格納している。パーソナルコンピュータ200の製造業者は、CAからCAの公開鍵PK_CAを入手し、パーソナルコンピュータ200が製造される際に、製造業者によりCAの公開鍵PK_CAが公開鍵格納部211へ書き込まれる。

[0059] デバイス鍵格納部204は、パーソナルコンピュータ200に割り当てられたデバイスDK$_j$を予め格納している。デバイスDK$_j$は、パーソナルコンピュータ200が製造される際に、製造業者によりデバイス鍵格納部204に書き込まれる。

(2)入出力部201

入出力部201は、パーソナルコンピュータ200の他の構成要素による指示により、当該他の構成要素から情報を受け取り、受け取った情報をドライブ装置100へ出力する。また、ドライブ装置100から情報を受け取り、受け取った情報を、情報の内容に応じて、パーソナルコンピュータ200の他の構成要素へ出力する。

[0060] (3)比較更新部202

比較更新部202は、記録媒体300から、ドライブ装置100及び入出力部201を介して、リストD及びリストHのバージョン番号MVN301を受信し、最新リスト格納部206からリストHのバージョン番号HVNを読み出し、受信したバージョン番号MVNと読み出したバージョン番号HVNとの新旧を比較する。具体的には、バージョン番号MVNとバージョン番号HVNとの大小を比較し、数字が大きい方が新しいと判断する。バージョン番号HVNがバージョン番号MVNより古い場合に、最新リスト格納部206に格納されているリストHは古いと判断し、通信部203及びインターネット20を介して、認証局装置30と接続し、認証局装置30から、インターネット20及び通信部203を介して、最新版のリストH及び最新版のリストDを取得し、取得した最新版のリストHを最新リスト格納部206へ上書きし、取得した最新版のリストDを最新リスト格納部209へ上書きする。

[0061] (4)証明書送信部208

証明書送信部208は、証明書格納部207からパーソナルコンピュータ200の公開鍵証明書を読み出し、次に、最新リスト格納部206に格納されているリストHから、パーソナルコンピュータ200を識別するIDを含む区間、バージョン番号、それらに対する署名からなる部分リストを抽出し、読み出した公開鍵証明書と抽出した部分リストとを、入出力部201を介して、ドライブ装置100へ出力する。

[0062] 一例として、パーソナルコンピュータ200が公開鍵証明書のIDとして、「0007」を持つ場合には、証明書送信部208は、「0007」を含む区間である識別子HID$_3$ 504a

及び識別子HID_4 504bと、CAの署名データ508とを部分リストとして抽出する。

次に、証明書送信部208は、読み出した公開鍵証明書と抽出した部分リストとを、入出力部201を介して、ドライブ装置100へ出力する。

[0063] (5)検証部210

検証部210は、ドライブ装置100から、入出力部201を介して、ドライブ装置100の公開鍵証明書を受け取り、公開鍵格納部211からCAの公開鍵PK_CAを読み出し、読み出したCAの公開鍵PK_CAを用いて、ドライブ装置100の公開鍵証明書に対してCAが付与した署名の正当性を検証し、検証に失敗すると、以降の処理を中止する。検証に成功すると、さらに、受け取った公開鍵証明書と最新リスト格納部209に格納されているリストDとを用いて、受け取った公開鍵証明書が有効であるか否かを検証する。具体的には、受け取った公開鍵証明書から公開鍵の識別子を抽出し、抽出した公開鍵の識別子が、リストDに含まれているか否かを判断し、含まれていると判断する場合には、当該公開鍵証明書は、無効であると判断し、以降の処理を中止する。含まれていないと判断する場合には、当該公開鍵証明書は、有効であると判断する。検証部210は、その判断結果を公開鍵暗号処理部212へ出力する。

[0064] (6)公開鍵暗号処理部212

公開鍵暗号処理部212は、パーソナルコンピュータ200とドライブ装置100とを接続する汎用の通信路40上で情報を安全に送信するための認証付き通信路(SAC)を確立するのに必要な認証／鍵共有処理を実行する。前記鍵共有処理において、ドライブ装置100と共有するセッション鍵を生成する。

[0065] (7)復号部213

復号部213は、ドライブ装置100から、入出力部201を介して、二重暗号化コンテンツ鍵を受け取り、公開鍵暗号処理部212において生成されたセッション鍵を用いて、受け取った二重暗号化コンテンツ鍵に復号アルゴリズムを施して、暗号化コンテンツ鍵を生成し、生成した暗号化コンテンツ鍵を復号部214へ出力する。

[0066] (8)復号部205

復号部205は、記録媒体300から、ドライブ装置100及び入出力部201を介して、暗号化メディア鍵群を受信し、受信した暗号化メディア鍵群からパーソナルコンピュ

ータ200に対応する暗号化メディアを特定して抽出し、デバイス鍵格納部204からデバイス鍵DK_jを読み出し、読み出したデバイス鍵DK_jを用いて、抽出した暗号化メディア鍵に、復号アルゴリズムを施して、復号メディア鍵を生成し、生成した復号メディア鍵を復号部214へ出力する。

[0067] なお、ある特定の装置にだけメディア鍵を与える方法は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。その一例としては、木構造を利用して鍵を管理する技術が開示されている。

(9)復号部214

復号部214は、復号部213から暗号化コンテンツ鍵を受け取り、復号部205から復号メディア鍵を受け取り、受け取った復号メディア鍵を用いて、受け取った暗号化コンテンツ鍵に、復号アルゴリズムを施して、復号コンテンツ鍵を生成し、生成した復号コンテンツ鍵を復号部215へ出力する。

[0068] (10)復号部215

復号部215は、復号部214から復号コンテンツ鍵を受け取り、記録媒体300から、ドライブ装置100及び入出力部201を介して、暗号化コンテンツを受信し、受け取った前記コンテンツ鍵を用いて、受信した暗号化コンテンツに復号アルゴリズムを施して、復号コンテンツを生成し、生成した復号コンテンツを再生部216へ出力する。

[0069] (11)再生部216

再生部216は、復号部215から復号コンテンツを受け取り、受け取った復号コンテンツに、デコード、伸張などのアルゴリズムを施して、デジタルの映像データ及びデジタルの音声データを生成し、生成したデジタルの映像データ及びデジタルの音声データを、アナログの映像信号及びアナログの音声信号に変換し、映像信号及び音声信号をそれぞれ、モニタ217及びスピーカ218へ出力する。

[0070] 1.6 認証システム10の動作

(1)認証システム10の主要な動作

認証システム10の主要な動作について、図6ー図9に示すフローチャートを用いて、説明する。

パーソナルコンピュータ200の比較更新部202は、入出力部201を介して、バージ

ョン番号の読み出し指示を、ドライブ装置100へ出力する(ステップS101)。

[0071] ドライブ装置100の入出力部102が、バージョン番号の読み出し指示を受け取ると(ステップS101)、入出力部101は、記録媒体300からバージョン番号MVN301を読み出し(ステップS102)、入出力部102を介して、読み出したバージョン番号MVN301をパーソナルコンピュータ200へ出力する(ステップS103)。

パーソナルコンピュータの比較更新部202は、ドライブ装置100から入出力部201を介して、バージョン番号MVN301を受け取り(ステップS103)、次に、最新リスト格納部422からリストHのバージョン番号HVNを読み出し、受信したバージョン番号MVNと読み出したバージョン番号HVNとの新旧を比較する(ステップS104)。バージョン番号HVNがバージョン番号MVNより古い場合に(ステップS105)、通信部203及びインターネット20を介して、認証局装置30に対してリストH及びリストDを要求する(ステップS106)。

[0072] 次に、前記要求を受け取ると(ステップS106)、認証局装置30は、最新のリストH及び最新のリストDを読み出し(ステップS107)、インターネット20を介して、読み出した最新のリストH及び最新のリストDを、パーソナルコンピュータ200へ送信する(ステップS108)。

比較更新部202は、認証局装置30から、インターネット20及び通信部203を介して、最新のリストH及び最新のリストDを受け取り(ステップS108)、受け取った最新版のリストHを最新リスト格納部206へ上書きし(ステップS109)、受け取った最新版のリストDを最新リスト格納部209へ上書きする(ステップS110)。

[0073] 次に、証明書送信部208は、証明書格納部207からパーソナルコンピュータ200の公開鍵証明書を読み出し、次に、最新リスト格納部206に格納されているリストHから、パーソナルコンピュータ200を識別するIDを含む区間、バージョン番号、それらに対する署名からなる部分リストを抽出し(ステップS111)、読み出した公開鍵証明書と抽出した部分リストとを、入出力部201を介して、ドライブ装置100へ出力する(ステップS112)。

[0074] ドライブ装置100の検証部104は、パーソナルコンピュータ200から入出力部102を介して、部分リスト及び公開鍵証明書を受け取り(ステップS112)、公開鍵格納部1

03からCAの公開鍵PK__CAを読み出し、読み出した公開鍵PK__CAを用いて、受け取った部分リストに含まれる署名データに対して署名検証を施し、さらに、読み出した公開鍵PK__CAを用いて、受け取った公開鍵証明書に含まれる署名データに対して署名検証を施す(ステップS113)。両方の署名検証のいずれか一方において検証に失敗すると(ステップS114)、以降の処理を中止する。両方の署名検証に成功すると(ステップS114)、さらに、検証部104は、受け取った前記公開鍵証明書に含まれる識別子が、前記部分リストに含まれているか否かを判断する(ステップS115)。識別子が部分リストに含まれていない場合には(ステップS116)、前記公開鍵証明書は無効であると判断して、以降の処理を中止する。識別子が部分リストに含まれている場合には、前記公開鍵証明書は有効であると判断する(ステップS116)。次に、証明書送信部106は、証明書格納部105からドライブ装置100の公開鍵証明書を読み出し(ステップS117)、読み出した公開鍵証明書を入出力部102を介して、パーソナルコンピュータ200へ出力する(ステップS118)。

[0075] 次に、パーソナルコンピュータ200の検証部210は、ドライブ装置100から、入出力部201を介して、ドライブ装置100の公開鍵証明書を受け取り(ステップS118)、公開鍵格納部211からCAの公開鍵PK__CAを読み出し、読み出したCAの公開鍵PK__CAを用いて、ドライブ装置100の公開鍵証明書に対してCAが付与した署名の正当性を検証し(ステップS119)、検証に失敗すると(ステップS120)、以降の処理を中止する。検証に成功すると(ステップS120)、さらに、受け取った公開鍵証明書と最新リスト格納部209に格納されているリストDとを用いて、から受け取った公開鍵証明書が有効であるか否かを検証する(ステップS121)。無効であると判断する場合には(ステップS122)、以降の処理を中止する。有効であると判断する場合には(ステップS122)、パーソナルコンピュータ212の公開鍵暗号処理部212とドライブ装置100の公開鍵暗号処理部107とは、パーソナルコンピュータ200とドライブ装置100とを接続する汎用の通信路40上で情報を安全に送信するための認証付き通信路(SAC)を確立するのに必要な認証／鍵共有処理を実行する。前記鍵共有処理において、ドライブ装置100と共有するセッション鍵を生成する(ステップS124、ステップS123)。こうして、ドライブ装置100とパーソナルコンピュータ200との間では、両者の公開鍵

暗号化処理部が動作してSACを確立し、データの受け渡しはSACを介して安全に行われ、SAC処理の結果として、両者はセッション鍵を共有する。

[0076] 次に、パーソナルコンピュータ200の復号部213は、入出力部201を介して、ドライブ装置100に対して、暗号化コンテンツ鍵を要求する(ステップS130)。

ドライブ装置100の暗号化部108は、暗号化コンテンツ鍵の前記要求を受け取り(ステップS130)、入出力部101を介して、記録媒体300から暗号化コンテンツ鍵303を読み出し(ステップS131)、公開鍵暗号処理部405により生成されたセッション鍵を用いて、読み出した暗号コンテンツ鍵に暗号化アルゴリズムを施して、二重暗号化コンテンツ鍵を生成し(ステップS132)、生成した二重暗号化コンテンツ鍵を、入出力部102を介して、パーソナルコンピュータ200へ出力する(ステップS133)。

[0077] パーソナルコンピュータ200の復号部213は、ドライブ装置100から、入出力部201を介して、二重暗号化コンテンツ鍵を受け取り(ステップS133)、公開鍵暗号処理部212において生成されたセッション鍵を用いて、受け取った二重暗号化コンテンツ鍵に復号アルゴリズムを施して、暗号化コンテンツ鍵を生成し、生成した暗号化コンテンツ鍵を復号部214へ出力する(ステップS134)。次に、復号部205は、ドライブ装置100に対して、入出力部201を介して、暗号化メディア鍵の要求を出力する(ステップS135)。

[0078] 次に、ドライブ装置100の入出力部102は、暗号化メディア鍵の前記要求を受け取り(ステップS135)、入出力部101を介して、記録媒体300から暗号化メディア鍵群を読み出し(ステップS136)、読み出した暗号化メディア鍵群をパーソナルコンピュータ200へ出力する(ステップS107)。

次に、パーソナルコンピュータ200の復号部205は、記録媒体300から、ドライブ装置100及び入出力部201を介して、暗号化メディア鍵群を受信し(ステップS137)、受信した暗号化メディア鍵群からパーソナルコンピュータ200に対応する暗号化メディアを特定して抽出し、デバイス鍵格納部204からデバイス鍵DK_jを読み出し、読み出したデバイス鍵DK_jを用いて、抽出した暗号化メディア鍵に、復号アルゴリズムを施して、復号メディア鍵を生成し、生成した復号メディア鍵を復号部214へ出力する(ステップS138)。次に、復号部214は、復号部213から暗号化コンテンツ鍵を受け取

り、復号部205から復号メディア鍵を受け取り、受け取った復号メディア鍵を用いて、受け取った暗号化コンテンツ鍵に、復号アルゴリズムを施して、復号コンテンツ鍵を生成し、生成した復号コンテンツ鍵を復号部215へ出力する(ステップS139)。次に、復号部215は、ドライブ装置100に対して、入出力部201を介して、暗号化コンテンツの要求を出力する(ステップS140)。

[0079] 次に、ドライブ装置100の入出力部102は、パーソナルコンピュータ200から暗号化コンテンツの前記要求を受け取り(ステップS140)、入出力部101を介して、記録媒体300から暗号化コンテンツを読み出し(ステップS141)、読み出した暗号化コンテンツをパーソナルコンピュータ200へ出力する(ステップS142)。

次に、パーソナルコンピュータ200の復号部215は、記録媒体300から、ドライブ装置100及び入出力部201を介して、暗号化コンテンツを受信し(ステップS142)、復号部214から復号コンテンツ鍵を受け取り、受け取った前記コンテンツ鍵を用いて、受信した暗号化コンテンツに復号アルゴリズムを施して、復号コンテンツを生成し、生成した復号コンテンツを再生部216へ出力する(ステップS143)。次に、再生部216は、復号部215から復号コンテンツを受け取り、受け取った復号コンテンツに、デコード、伸張などのアルゴリズムを施して、デジタルの映像データ及びデジタルの音声データを生成し、生成したデジタルの映像データ及びデジタルの音声データを、アナログの映像信号及びアナログの音声信号に変換し、映像信号及び音声信号をそれぞれ、モニタ217及びスピーカ218へ出力する。モニタ217は、映像信号から映像を生成して表示し、スピーカ218は、音声信号から音声を生成して出力する(ステップS144)。

[0080] (2)SACの動作

次に、ドライブ装置100とパーソナルコンピュータ200との間で設定されるSACの実現の動作について、図10に示すフローチャートを用いて説明する。

ただし、Sign( )を署名生成関数、Veri( )を署名検証関数、Gen( )を鍵生成関数とし、Yをそのシステム固有のシステムパラメータとする。

[0081] また、鍵生成関数Gen( )は、

Gen(x, Gen(y, z)) =Gen(y, Gen(x, z))の関係を満たすものとする。

なお、このような鍵生成関数は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。その一例としては、ディフィーヘルマン(DH)型公開鍵配送法がある。

[0082] 公開鍵暗号処理部107は、CAが発行した証明書Cert__Aを内部から読み出し(ステップS201)、読み出した証明書Cert__Aを公開鍵暗号処理部212に送信する(ステップS202)。ここでは、証明書Cert__Aは、ドライブ装置100の公開鍵PK__A、ドライブ装置100の識別子ID__A、それらに対するCAの署名データSig__CAから構成されている。

[0083] 公開鍵暗号処理部212は、CAの公開鍵P__CAを用いて証明書Cert__Aに付与されている署名データSig__CAが正しいか否かを検証する(ステップS203)。検証結果が正しくない場合、SACの設定処理を終了する。さらに、公開鍵暗号処理部212は、ドライブ装置100の識別子ID__Aが、CRLに登録されているか否かを確認する(ステップS204)。登録されている場合は、SACの設定処理を終了する。

[0084] 公開鍵暗号処理部212は、CAが発行した証明書Cert__Bを内部から読み出し(ステップS205)、読み出した証明書Cert__Bを公開鍵暗号処理部107に送信する(ステップS206)。ここでは、証明書Cert__Bは、パーソナルコンピュータ200の公開鍵PK__B、パーソナルコンピュータ200の識別子ID__B、それらに対するCAの署名Sig__CAから構成されている。

[0085] 公開鍵暗号処理部107は、CAの公開鍵P__CAを用いてCert__Bに付与されている署名Sig__CAが正しいか否かを検証する(ステップS207)。検証結果が正しくない場合、SACの設定処理を終了する。さらに、公開鍵暗号処理部107は、パーソナルコンピュータ200の識別子ID__Bが、CRLに登録されているか否かを確認する(ステップS208)。登録されている場合は、SACの設定処理を終了する。

[0086] 公開鍵暗号処理部107は、乱数Cha__Aを生成し(ステップS209)、乱数Cha__Aを公開鍵暗号処理部212に送信する(ステップS210)。

公開鍵暗号処理部212は、受信したCha__Aに対して、自身の秘密鍵SK__Bで署名データSig__Bを生成し(ステップS211)、署名データSig__Bを公開鍵暗号処理部107に送信する(ステップS212)。

[0087] 公開鍵暗号処理部107は、S206で受信した公開鍵暗号処理部212の公開鍵PK__Bを用いて、Sig__Bが正しいか否かを検証する(ステップS213)。検証結果が正しくない場合、SACの設定処理を終了する。

公開鍵暗号処理部212は、乱数Cha__Bを生成し(ステップS214)、乱数Cha__Bを公開鍵暗号処理部107に送信する(ステップS215)。

[0088] 公開鍵暗号処理部107は、受信したCha__Bに対して、自身の秘密鍵SK__Aで署名データSig__Aを生成し(ステップS216)、署名データSig__Aを公開鍵暗号処理部212に送信する(ステップS217)。

公開鍵暗号処理部212は、S202で受信した公開鍵暗号処理部107の公開鍵PK__Aを用いて、署名データSig__Aが正しいか否かを検証する(ステップS218)。検証結果が正しくない場合、SACの設定処理を終了する。

[0089] 公開鍵暗号処理部212は、乱数bを生成し(ステップS219)、Key__B＝Gen(b, Y)を計算し(ステップS220)、Key__Bを公開鍵暗号処理部107に送信する(ステップS221)。

公開鍵暗号処理部107は、乱数aを生成し(ステップS222)、Key__A＝Gen(a, Y)を計算し(ステップS223)、Key__Aを公開鍵暗号処理部212に送信する(ステップS224)。さらに、公開鍵暗号処理部107は、両者で共有する鍵Key__AB＝Gen(b, Key__A)を算出する(ステップS226)。

[0090] 公開鍵暗号処理部212は、両者で共有する鍵Key__AB＝Gen(a, Key__B)を算出する(ステップS225)。

こうして、公開鍵暗号処理部107及び公開鍵暗号処理部212は、鍵Key__ABを共有することができる。

1．7 まとめ

以上に示したように、パーソナルコンピュータ200の保持するリストHが古い場合、リストHを更新しなければ、パーソナルコンピュータ200は、ドライブ装置100によって認証されないため、この仕組みは、パーソナルコンピュータ200による自身のリストHの更新を促し、強制化することができる。その際に、リストDも合わせて更新することにより、本来強制力の働かないリストDの更新も行うことが可能となる。

[0091] 2. 第2の実施の形態

本願の発明の別の実施の形態としての認証システム10b(図示していない)について説明する。

2. 1 認証システム10bの構成

認証システム10bは、認証システム10と同様に、ドライブ装置100、パーソナルコンピュータ200b及び認証局装置30b(図示していない)から構成されている。ドライブ装置100には、記録媒体300が装着される。

[0092] 認証システム10では、公開鍵証明書の有効又は無効を示すために、無効化された公開鍵証明書の識別子から構成されるリストD及び有効な公開鍵証明書の識別子から構成されるリストHが利用される。これに対して、認証システム10bでは、リストD及びリストHを統合して構成され、無効化された公開鍵証明書の識別子及び有効な公開鍵証明書の識別子から構成される証明書識別子リストが利用される。この点において、認証システム10bと認証システム10とは相違する。

[0093] ここでは、主として、認証システム10との相違点を中心として説明する。

認証システム10bのドライブ装置100及び記録媒体300は、それぞれ、認証システム10のドライブ装置100及び記録媒体300と同じ構成を有しているので、ドライブ装置100及び記録媒体300についての説明は、省略する。

なお、記録媒体300が記録しているバージョン番号MVN301は、記録媒体300に記録されているデータを利用する際に適用されるべき証明書識別子リストの世代を示す番号である。

[0094] 2. 2 パーソナルコンピュータ200bの構成

パーソナルコンピュータ200bは、パーソナルコンピュータ200と同様の構成を有し、図11に示すように、入出力部201、システムLSI230b、通信部203、再生部216、制御部221及び図示していない他の構成要素から構成される。

なお、パーソナルコンピュータ200bは、具体的には、前記システムLSI、マイクロプロセッサ、ROM、RAM、バス、ハードディスクユニット、通信ユニットなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータ

プログラムに従って動作することにより、パーソナルコンピュータ200bは、その一部の機能を達成する。

[0095] パーソナルコンピュータ200bが有する入出力部201、通信部203、再生部216、制御部221及び他の構成要素は、それぞれ、パーソナルコンピュータ200が有する入出力部201、通信部203、再生部216、制御部221及び他の構成要素と同一である。

システムLSI230bは、図11に示すように、比較更新部202b、最新リスト格納部206b、証明書格納部207、証明書送信部208b、検証部210b、公開鍵格納部211、公開鍵暗号処理部212、復号部213、復号部214及び復号部215から構成されている。

[0096] システムLSI230bが有する証明書格納部207、公開鍵格納部211、公開鍵暗号処理部212、復号部213、復号部214及び復号部215は、それぞれ、システムLSI230が有する証明書格納部207、公開鍵格納部211、公開鍵暗号処理部212、復号部213、復号部214及び復号部215と同一である。

ここでは、比較更新部202b、最新リスト格納部206b、証明書送信部208b、検証部210bについて説明する。

[0097] (1)最新リスト格納部206b

最新リスト格納部206bは、予め、公開鍵証明書の有効性及び無効性を示す証明書識別子リスト600を格納している。

パーソナルコンピュータ200bの製造業者は、CAから証明書識別子リスト600を入手し、パーソナルコンピュータ200bが製造される際に、製造業者により証明書識別子リスト600が最新リスト格納部206bへ書き込まれる。

[0098] 証明書識別子リスト600は、図12に一例として示すように、ドライブ装置100が保持する公開鍵証明書のうち、識別子ID＝1、ID＝2の2つの公開鍵証明書が無効化され、他の公開鍵証明書が有効であり、パーソナルコンピュータ200bが保持する公開鍵証明書のうち、識別子ID＝9、ID＝13ー16の5つの公開鍵証明書が無効化され、他の公開鍵証明書が有効である場合の例を示している。

[0099] また、この図の参照符号620により示される枠内に、各識別子を表示しており、×印

が付された番号は、無効化された公開鍵証明書の識別子を示している。×印が付されていない番号は、無効化されていない公開鍵証明書の識別子を示している。枠620において、×印が付された番号の最初の区間620aは、識別子の集合{1、2}から構成され、×印が付されていない番号の次の区間620bは、識別子の集合{3、4、5}から構成されている。また、×印が付されていない番号の次の区間620cは、識別子の集合{6、7、8}から構成され、×印が付された番号の次の区間620dは、識別子の集合{9}から構成され、×印が付されていない番号の次の区間620eは、識別子の集合{10、11、12}から構成され、×印が付された番号の次の区間620fは、識別子の集合{13、14、15、16}から構成され、×印が付されていない番号の次の区間620gは、識別子の集合{17、18、・・・}から構成されている。

[0100] 証明書識別子リスト600は、図12に示すように、バージョン番号フィールド601、識別子数フィールド602、無効化識別子フィールド613、組数フィールド605、有効識別子フィールド614、署名フィールド615から構成されている。

バージョン番号フィールド601には、バージョン番号VN601aが格納されており、識別子数フィールド602には、識別子数602aが格納されており、無効化識別子フィールド613には、2個の無効化識別子ID_1 603a、ID_2 604aが格納されており、組数フィールド605には、組数605aが格納されており、有効識別子フィールド614には、6個の識別子ID_3 606a、ID_4 606b、ID_5 607a、ID_6 607b、ID_7 608a、ID_8 608bが格納されており、署名フィールド615には、4個の署名データ609a、610a、611a、612aが格納されている。

[0101] ここで、バージョン番号VN601aは、証明書識別子リスト600の世代を示す番号であり、図12に示す例では、「0003」である。

識別子数602aは、無効化識別子フィールド613に格納されている無効化識別子の数を示しており、図12に示す例では、「0002」である。

無効化識別子ID_1 603a、ID_2 604aは、無効化すべき公開鍵証明書の識別番号を示し、図12に示す例では、「0001」、「0002」である。

[0102] 組数605aは、有効な公開鍵証明書の識別子が連続する区間の数を示しており、図12に示す例では、「0003」であり、区間が3個存在することを示している。

2個の識別子606a、606bは、組606を構成し、2個の識別子607a、607bは、組607を構成し、2個の識別子608a、608bは、組608を構成している。各組は、有効な公開鍵証明書の識別子が連続する区間の先頭の識別子と最後の識別子から構成される。

[0103] 図12に示す例では、組606は、識別子「0006」を先頭とし、識別子「0008」を最後とする区間620cを示しており、組607は、識別子「0010」を先頭とし、識別子「0012」を最後とする区間620eを示しており、組608は、識別子「0017」を先頭とし、識別子「9999」を最後とする区間620gを示している。

署名データ609は、組606に対応し、署名データ610は、組607に対応し、署名データ611は、組608に対応し、署名データ612は、証明書識別子リスト600の全体に対応している。

[0104] 4個の署名データ609ー612は、それぞれ、CAにより生成され、3個の署名データ609ー611は、それぞれ、証明書識別子リスト600に含まれ、対応する各組のデータの正当性を検証するための署名データであり、署名データ612は、証明書識別子リスト600に含まれ当該署名データ612を除く他のデータの正当性を検証するための署名データである。

[0105] 署名データ609は、CAの秘密鍵SK_CAを用いて、バージョン番号VN601aと、組606に含まれている識別子ID_3 606aと、識別子ID_4 606bとをこの順序で、連結して生成される連結データに、デジタル署名アルゴリズムSigを施して生成されたものである。

CAの署名データSig_1

$=Sig(SK\_CA, VN||ID_3||ID_4)$

署名データ610は、CAの秘密鍵SK_CAを用いて、バージョン番号VN601aと、組607に含まれている識別子ID_5 607aと、識別子ID_6 607bとをこの順序で、連結して生成される連結データに、デジタル署名アルゴリズムSigを施して生成されたものである。

[0106] CAの署名データSig_2

$=Sig(SK\_CA, VN||ID_5||ID_6)$

署名データ611は、CAの秘密鍵SK_CAを用いて、バージョン番号VN601aと、組608に含まれている識別子ID_7 608aと、識別子ID_8 608bとをこの順序で、連結して生成される連結データに、デジタル署名アルゴリズムSigを施して生成されたものである。

[0107] CAの署名データSig_3

$=Sig(SK\_CA, VN||ID_7||ID_8)$

署名データ612は、CAの秘密鍵SK_CAを用いて、バージョン番号VN601aと、識別子ID_1 603aと、識別子ID_2 604aと、識別子ID_3 606aと、識別子ID_4 606bと、識別子ID_5 607aと、識別子ID_6 607bと、識別子ID_7 608aと、識別子ID_8 608bと、署名データ609と、署名データ610と、署名データ611とをこの順序で、連結して生成される連結データに、デジタル署名アルゴリズムSigを施して生成されたものである。

[0108] CAの署名データ

$=Sig(SK\_CA, VN||ID_1||ID_2||ID_3||ID_4||ID_5||ID_6||ID_7||ID_8||Sig_1||Sig_2||Sig_3)$

なお、前記署名データは、必ずしも複数のデータの連結値から生成される必要はなく、複数のデータの連結値のハッシュ値から生成される形態であってもよい。さらに、前記署名は、付録型の署名である必要はなく、署名検証実施後、署名対象データが生成される回復型の署名であってもよい。その場合、証明書識別子リストには無効化識別子フィールド及び有効化識別子フィールドがなく、検証時に署名から各IDが生成される。

[0109] (2)比較更新部202b

比較更新部202bは、記録媒体300から、ドライブ装置100及び入出力部201を介して、証明書識別子リストのバージョン番号MVN301を受信し、最新リスト格納部206bから証明書識別子リスト600のバージョン番号VNを読み出し、受信したバージョン番号MVNと読み出したバージョン番号VNとの新旧を比較する。具体的には、バージョン番号MVNとバージョン番号VNとの大小を比較し、数字が大きい方が新しいと判断する。バージョン番号VNがバージョン番号MVNより古い場合に、最新リスト

格納部206bに格納されている証明書識別子リストは古いと判断し、通信部203及びインターネット20を介して、認証局装置30bと接続し、認証局装置30bから、インターネット20及び通信部203を介して、最新版の証明書識別子リストを取得し、取得した最新版の証明書識別子リストを最新リスト格納部206bへ上書きする。

[0110] (3)証明書送信部208b

証明書送信部208bは、証明書格納部207からパーソナルコンピュータ200の公開鍵証明書を読み出し、次に、最新リスト格納部206bに格納されている証明書識別子リストから、パーソナルコンピュータ200bを識別するIDを含む区間、バージョン番号、それらに対する署名からなる部分リストを抽出し、読み出した公開鍵証明書と抽出した部分リストとを、入出力部201を介して、ドライブ装置100へ出力する。

[0111] 一例として、パーソナルコンピュータ200が公開鍵証明書のIDとして、「0007」を持つ場合には、証明書送信部208bは、「0007」を含む区間を示す識別子ID_3 606a及び識別子ID_4 606bと、CAの署名データ509とを部分リストとして抽出する。

次に、証明書送信部208は、読み出した公開鍵証明書と抽出した部分リストとを、入出力部201を介して、ドライブ装置100へ出力する。

[0112] (4)検証部210b

検証部210bは、ドライブ装置100から、入出力部201を介して、ドライブ装置100の公開鍵証明書を受け取り、公開鍵格納部211からCAの公開鍵PK_CAを読み出し、読み出したCAの公開鍵PK_CAを用いて、ドライブ装置100の公開鍵証明書に対してCAが付与した署名の正当性を検証し、検証に失敗すると、以降の処理を中止する。検証に成功すると、さらに、受け取った公開鍵証明書と最新リスト格納部206bに格納されている証明書識別子リストとを用いて、受け取った公開鍵証明書が有効であるか否かを検証する。具体的には、受け取った公開鍵証明書から公開鍵の識別子を抽出し、抽出した公開鍵の識別子が、証明書識別子リストに含まれているか否かを判断し、含まれていると判断する場合には、当該公開鍵証明書は、無効であると判断し、以降の処理を中止する。含まれていないと判断する場合には、当該公開鍵証明書は、有効であると判断する。検証部210bは、その判断結果を公開鍵暗号処理部212へ出力する。

[0113] 2. 3 認証システム10bの動作

認証システム10bの動作は、認証システム10の主要な動作と類似しており、図6ー図9に示すフローチャートに従うものであるが、ここでは、認証システム10の主要な動作との相違点を中心として説明する。

ステップS104において、比較更新部202bは、記録媒体300から読み出した証明書識別子リストのバージョン番号MVN301と、最新リスト格納部206bから読み出した証明書識別子リスト600のバージョン番号VNとを比較する。

[0114] バージョン番号VNがバージョン番号MVNより古い場合に(ステップS105)、ステップS108において、認証局装置30bから、インターネット20及び通信部203を介して、最新版の証明書識別子リストを取得し、ステップS109、ステップS110において、取得した最新版の証明書識別子リストを最新リスト格納部206bへ上書きする。

[0115] ステップS111において、証明書送信部208bは、最新リスト格納部206bに格納されている証明書識別子リストから、パーソナルコンピュータ200bを識別するIDを含む区間、バージョン番号、それらに対する署名からなる部分リストを抽出し、読み出した公開鍵証明書と抽出した部分リストとを、入出力部201を介して、ドライブ装置100へ出力する。

[0116] また、ステップS121において、検証部210bは、受け取った公開鍵証明書と最新リスト格納部206bに格納されている証明書識別子リストとを用いて、受け取った公開鍵証明書が有効であるか否かを検証する。

3. その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

[0117] (1)上記の実施の形態1では、無効化された公開鍵証明書の識別子を含むリストD400と、有効な公開鍵証明書の識別子を含むリストH500とを利用し、上記の実施の形態2では、無効化された公開鍵証明書の識別子と、有効な公開鍵証明書の識別子を含む証明書識別子リスト600を利用するとしているが、本発明はこれらの構成に限定されるものではない。

[0118] 例えば、リストD400、リストH500及び証明書識別子リストとは、別のデータ構造を有する証明書識別子リスト700は、図13に示すように、バージョン番号フィールド730、無効又は有効な識別子を示すフィールド731、無効又は有効な識別子を示すフィールド732、無効又は有効な識別子の区間を示すフィールド733、署名フィールド734から構成されている。

[0119] また、この図の参照符号721により示される枠内に、各識別子を表示しており、×印が付された番号は、無効化された公開鍵証明書の識別子を示している。×印が付されていない番号は、無効化されていない公開鍵証明書の識別子を示している。

枠721において、各識別子は、3個の範囲722、723、724に区分されている。範囲722は、識別子の集合{1、2、・・・、8}から構成され、範囲723は、識別子の集合{9、10、・・・、16}から構成され、範囲724は、識別子の集合{17、18、・・・、9999}から構成されている。

[0120] 範囲722において、識別子725、726が無効化され、範囲723において、識別子727、728が有効であり、範囲724において、集合{18、・・・、9999}に含まれる識別子が有効である。

フィールド731、フィールド732及びフィールド733は、それぞれ、範囲722、723、724に対応している。

[0121] バージョン番号フィールド730には、リストD400、リストH500及び証明書識別子リストと同様に、証明書識別子リスト700の世代を示すバージョン番号701aが格納している。

フィールド731には、区分Flag741、範囲情報702、識別子数703、識別子ID_1 704及び識別子ID_2 705が格納されている。

[0122] 区分Flag741は、2桁の数字から構成され、「00」、「01」、「10」及び「11」のいずれかの値をとる。「00」は、フィールド731が無効化された識別子を個々に示すものであることを表現しており、「01」は、フィールド731が無効化された識別子の範囲を示すものであることを表現しており、「10」は、フィールド731が有効な識別子を個々に示すものであることを表現しており、「11」は、フィールド731が有効な識別子の範囲を示すものであることを表現している。

[0123] 区分741は、「00」であるので、フィールド731は、無効化された識別子を個々に示している。

範囲情報702は、フィールド731に含まれる情報が示す識別子の範囲722を示し、当該範囲の先頭識別子と最終識別子とから構成される。この図に示す例では、範囲情報702は、「0001:0008」であり、これは、識別子「0001」を先頭とし、識別子「0008」を最終とする範囲を示している。

[0124] 識別子数703は、前記の範囲に含まれる無効化された識別子の数を示す。この図に示す例では、識別子数703は、「0002」であり、これは、無効化された識別子が2個存在することを示している。

識別子ID_1 704及び識別子ID_2 705は、無効化された識別子を示している。

フィールド732には、区分Flag742、範囲情報706、識別子数707、識別子ID_3 708及び識別子ID_4 709が格納されている。

[0125] 区分Flag742は、区分Flag741と同様である。ここで、区分Flag742は、「10」であるので、フィールド732は、有効な識別子を個々に示す。

範囲情報706は、フィールド732に含まれる情報が示す識別子の範囲723を示し、当該範囲の先頭識別子と最終識別子とから構成される。この図に示す例では、範囲情報706は、「0009:0016」であり、これは、識別子「0009」を先頭とし、識別子「0016」を最終とする範囲を示している。

[0126] 識別子数707は、前記の範囲に含まれる有効な識別子の数を示す。この図に示す例では、識別子数707は、「0002」であり、これは、有効な識別子が2個存在することを示している。

識別子ID_3 708及び識別子ID_4 709は、有効な識別子を示している。

フィールド733には、区分Flag743、範囲情報710、組数711、識別子ID_5 712a及び識別子ID_6 712bが格納されている。

[0127] 区分Flag743は、区分Flag741と同様である。ここで、区分Flag743は、「11」であるので、フィールド732は、有効な識別子の範囲を示す。

範囲情報710は、フィールド733に含まれる情報が示す識別子の範囲724を示し、当該範囲724の先頭識別子と最終識別子とから構成される。この図に示す例では、

範囲情報710は、「0017:9999」であり、これは、識別子「0017」を先頭とし、識別子「9999」を最終とする範囲を示している。

[0128] 組数711は、前記の範囲に含まれる有効な識別子の区間の数を示す。この図に示す例では、組数711は、「0001」であり、これは、有効な識別子の区間が1個存在することを示している。

識別子ID_5 712a及び識別子ID_6 712bは、前記有効な識別子の区間の先頭と最終を示している。この図に示す例では、「0018」及び「9999」であり、「0018」及び「9999」は、有効な識別子の区間の先頭の識別子が「0018」であり、最終の識別子が「9999」であることを示している。

[0129] 署名フィールド734には、CAの署名データ713、714及び715が格納され、署名データ713、714及び715は、それぞれ、フィールド731、732及び733に対応している。

署名データ713は、CAの秘密鍵SK_CAを用いて、区分Flag741と、範囲情報702に含まれる2個の識別子と、バージョン番号VN701と、識別子ID_1 704と、識別子ID_2 705とをこの順序で、連結して生成される連結データに、デジタル署名アルゴリズムSigを施して生成されたものである。

[0130] CAの署名データSig_1

$=Sig(SK\#CA、Flag||0001||0008||VN||ID_1||ID_2)$

署名データ714は、CAの秘密鍵SK_CAを用いて、区分Flag742と、範囲情報706に含まれる2個の識別子と、バージョン番号VN701と、識別子ID_3 708と、識別子ID_4 709とをこの順序で、連結して生成される連結データに、デジタル署名アルゴリズムSigを施して生成されたものである。

[0131] CAの署名データSig_2

$=Sig(SK\#CA、Flag||0009||0016||VN||ID_3||ID_4)$

署名データ715は、CAの秘密鍵SK_CAを用いて、区分Flag743と、範囲情報710に含まれる2個の識別子と、バージョン番号VN701と、識別子ID_5 712aと、識別子ID_6 712bとをこの順序で、連結して生成される連結データに、デジタル署名アルゴリズムSigを施して生成されたものである。

[0132] CAの署名データSig_3

＝Sig(SK#CA、Flag||0017||9999||VN||ID_5 ||ID_6)

(2)リストDは、次に示すように構成されるとしてもよい。

別のデータ構造を有する証明書識別子リスト800は、図14に示すように、バージョン番号フィールド841、無効な識別子を示すフィールド842及び署名フィールド843から構成されている。

[0133] また、この図の参照符号820により示される枠内に、各識別子を表示しており、×印が付された番号は、無効化された公開鍵証明書の識別子を示している。×印が付されていない番号は、無効化されていない公開鍵証明書の識別子を示している。

枠820において、識別子821、822、823が無効化され、区間824に含まれる識別子が無効化され、識別子825が無効化されている。

[0134] バージョン番号フィールド841には、証明書識別子リスト800の世代を示すバージョン番号VN801が格納されている。

フィールド841には、区分Flag803aと識別子ID_1 803b、区分Flag804aと識別子ID_1 804b、区分Flag805aと識別子ID_1 805b、区分Flag806aと識別子ID_1 806b、区分Flag807aと識別子ID_1 807b及び区分Flag808aと識別子ID_1 808bが格納されている。

[0135] 区分Flag803aと識別子ID_1 803bとは、対応しており、区分Flag803aは、対応する識別子ID_1 803bが個々の識別子を示すか、又は区間の先頭の識別子及び最終の識別子のいずれかを示すものである。区分Flag803aの値が「0」であるときには、対応する識別子ID_1 803bは、個々の識別子を示し、区分Flag803aの値が「1」であるときには、対応する識別子ID_1 803bは、区間の先頭の識別子及び最終の識別子のいずれかを示す。この図において、区分Flag803aは、「0」であるので、識別子ID_1 803bは、個々の識別子を示している。

[0136] 他の区分Flagと識別子についても同様である。

この図において、区分Flag806a及び807bは、それぞれ、「1」であるので、識別子ID_1 806b及び807bは、それぞれ、区間の先頭の識別子及び最終の識別子を示している。つまり、識別子ID_1 806b及び807bは、それぞれ、「0013」および「0015」で

あるので、「0013」ー「0015」の区間に含まれる識別子は、全て無効化されている。

[0137] このように、証明書識別子リスト800は、識別子に対応して区分を有しており、この区分により、対応する識別子が個々のものか、または区間の先頭及び最終にいずれかを示すものかを表している。

(3) 上記の実施の形態1及び実施の形態2では、記録媒体は、予め暗号化されたコンテンツが記録されているDVD−Videoのようなプリレコーディッドメディアであるとしているが、本発明は、このような構成に限定されるものではない。

[0138] 例えば、記録媒体は、DVD−RAMのようなレコーダブルメディアであってもよい。その場合、実施の形態1及び実施の形態2と同様に認証を実行した後で、パーソナルコンピュータ200により、暗号化されたコンテンツが記録媒体に記録される。実施の形態1及び実施の形態2において、パーソナルコンピュータ200は、再生装置の役割を果たしているが、このように、記録装置の役割を果たすとしてもよい。

[0139] また、前記記録媒体は、例えば、フレキシブルディスク、ハードディスク、CD−ROM、MO、DVD−ROM、DVD−RAM、BD(Blu−ray Disc)、可搬型の半導体メモリなどであるとしてもよい。

(4) 上記の実施の形態1及び実施の形態2では、記録媒体にはバージョン番号のみが記録されている形態としたが、本発明は、このような構成に限定されるものではない。例えば、記録媒体には、バージョン番号と共に、最新リストも記録されており、記録媒体に記録されている最新リストを利用して、パーソナルコンピュータが自身が保持しているリストを更新するとしてもよい。

[0140] (5) 上記の実施の形態1及び実施の形態2において、ドライブ装置が、リストのバージョン番号を格納する格納部を有する構成であってもよい。この場合、ドライブ装置は、記録媒体から読み出したバージョン番号と、自身が保持するバージョン番号を比較して、新しいバージョン番号をパーソナルコンピュータに送信する構成であってもよい。

さらに、ドライブ装置が、リストのバージョン番号に加え、リスト自身を格納する格納部を有する構成であってもよい。この場合、ドライブ装置は、記録媒体から読み出したバージョン番号と、自身が保持するバージョン番号を比較して、自身が保持するバ

ージョン番号が新しければ、保持するバージョン番号、並びにリストを再生装置に送信する構成であってもよい。

[0141] (6)上記の実施の形態1及び実施の形態2では、認証に用いるデータ、及びコンテンツが記録媒体に記録される形態としたが、本発明はその構成に限定されるものではない。記録媒体の代わりに通信媒体を利用して、通信媒体を介して、認証に用いるデータ、及びコンテンツを受け渡しする構成であってもよい。また、記録媒体及び通信媒体を併用する形態であってもよい。

[0142] (7)上記の実施の形態1及び実施の形態2では、認証に用いるデータの保護にCAの署名を用いる形態としたが本発明はその構成に限定されるものではない。例えば、ドライブ装置は、当該ドライブ装置専用の秘密鍵を保持し、パーソナルコンピュータは、当該パーソナルコンピュータ専用の秘密鍵を用いる構成として、認証に用いるデータには、各秘密鍵を利用して生成された認証子を付与する構成であってもよい。

[0143] (8)上記の実施の形態1及び実施の形態2において、システムLSIに代えて、例えばパーソナルコンピュータにインストールされるコンピュータプログラムを記憶しており、コンピュータプログラムに従って、パーソナルコンピュータが備えるプロセッサが動作するとしてもよい。

このコンピュータプログラムは、暗号化コンテンツを復号して再生するプログラムであるが、コンテンツを暗号化して記録媒体に書き込む記録用ソフトウェアであってもよい。

[0144] (9)上記の実施の形態1及び実施の形態2において、パーソナルコンピュータ及びドライブ装置の代わりに、ドライブ部を一体として備えるDVD再生装置により実現するとしてもよい。DVD再生装置は、パーソナルコンピュータとドライブ装置とを含んで構成される。また、DVD再生装置に代えて、DVD記録装置であるとしてもよい。

また、パーソナルコンピュータの代わりに、デジタルTV表示装置を備え、ドライブ装置の代わりに、セットトップボックスつまりデジタル放送受信装置を備えるとしてもよい。

[0145] デジタルTV表示装置は、デジタル放送受信装置から放送されたバージョン番号を取得し、内部に記憶しているバージョン番号と、放送により取得したバージョン番号を

比較することにより、ホワイトリストを更新するか否かを判定し、更新すると判定する場合に、最新版のホワイトリストを取得し、自身が保持しているホワイトリストを最新版のホワイトリストに更新するとともに、最新版のブラックリストを取得し、保持しているブラックリストを取得した最新版のブラックリストに更新する。

[0146] デジタルTV表示装置は、ホワイトリストを用いて、自身の有効性を証明し、ブラックリストを用いて、デジタル放送受信装置の無効性を判断する。また、デジタル放送受信装置は、ブラックリストを用いて、デジタルTV表示装置の無効性を判断する。

デジタルTV表示装置及びデジタル放送受信装置が、相互に相手の有効性が確認できた場合に、デジタル放送受信装置は、デジタル放送により受信した暗号化コンテンツをデジタルTV表示装置へ出力し、デジタルTV表示装置は、暗号化コンテンツを復号してコンテンツを表示する。

[0147] また、上記の実施の形態1及び実施の形態2において、各携帯電話に代えて、携帯型の情報通信端末を用いるとしてもよい。

(10) 上記の実施の形態において、バージョン番号は、数値で示され、数値が大きいほど、新しい世代であるとしているが、これには限定されない。数値が大きいほど古い世代であるとしてもよい。

[0148] また、上記の実施の形態において、バージョン番号の大小を比較することにより、2つのリストの新旧を比較するとしているが、これには限定されない。例えば、2つのリストの生成された日付及び時刻を比較することにより、2つのリストの新旧を比較するとしてもよい。ここで、前記日付及び時刻も、バージョン番号と同様に、各リストの世代を示す情報であるといえる。

[0149] また、パーソナルコンピュータが、インターネットを介して、他のサーバ装置にデジタル情報の提供を依頼するときに、前記サーバ装置がパーソナルコンピュータに対して、ホワイトリストの更新を、前記デジタル情報の提供の条件としてもよい。このとき、前記サーバ装置は、パーソナルコンピュータに対して、ホワイトリストの更新を要求し、パーソナルコンピュータは、前記要求に従って、最新のホワイトリストを取得して更新する。その後、サーバ装置は、パーソナルコンピュータに対してデジタル情報を提供する。

（11）本発明は、認証用データの付帯情報を記録する記録媒体と、前記記録媒体から前記付帯情報を読み出す読出装置と、前記記録媒体を利用する端末装置からなる認証システムである。

[0150] 前記端末装置は、複数の認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して複数の認証用データを入手して前記格納部のデータを更新する。

ここで、前記複数の認証用データのうち少なくとも1つは、前記端末装置自身の有効性を前記読出装置に提示するための認証用データであり、さらに、前記認証用データのうち少なくとも1つは、前記読出装置の有効性を検証するための認証用データであるとしてもよい。

[0151] ここで、前記端末装置はさらに、前記端末装置自身の有効性を前記読出装置に提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する装置部を備え、前記読出装置はさらに、前記部分認証用データを受信する受信部を備えるとしてもよい。

ここで、前記読出装置はさらに、認証用データの付帯情報を格納する格納部と、前記記録媒体から読み出した付帯情報と前記格納する付帯情報を比較する比較部と、データを送信する送信部を備え、比較した結果、前記格納する付帯情報が新しいと判断した場合は、前記格納する付帯情報を前記端末装置に送信するとしてもよい。

[0152] ここで、前記読出装置はさらに、認証用データを格納する格納部と、前記記録媒体から読み出した付帯情報と前記格納する認証用データの付帯情報を比較する比較部と、データを送信する送信部を備え、比較した結果、前記格納する認証用データの付帯情報が新しいと判断した場合は、前記格納する認証用データを前記端末装置に送信するとしてもよい。

[0153] ここで、前記記録媒体が、認証用データ自身も記録するとしてもよい。

ここで、前記記録媒体の代わりに通信媒体を利用するとしてもよい。

また、本発明は、認証用データの付帯情報を記録する記録媒体と、前記記録媒体

から前記付帯情報を読み出す読出装置と、前記記録媒体を利用する端末装置からなる認証システムである。

[0154] 前記端末装置は、1つの認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して前記認証用データを入手して前記格納部のデータを更新し、前記認証用データは、前記端末装置自身の有効性を前記読出装置に提示するための認証用データであり、さらに、前記認証用データは、前記読出装置の有効性を検証するための認証用データも含む。

[0155] ここで、前記端末装置はさらに、前記端末装置自身の有効性を前記読出装置に提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する装置部を備え、前記読出装置はさらに、前記部分認証用データを受信する受信部を備えるとしてもよい。

ここで、前記読出装置はさらに、認証用データの付帯情報を格納する格納部と、前記記録媒体から読み出した付帯情報と前記格納する付帯情報を比較する比較部と、データを送信する送信部を備え、比較した結果、前記格納する付帯情報が新しいと判断した場合は、前記格納する付帯情報を前記端末装置に送信するとしてもよい。

[0156] ここで、前記読出装置はさらに、認証用データを格納する格納部と、前記記録媒体から読み出した付帯情報と前記格納する認証用データの付帯情報を比較する比較部と、データを送信する送信部を備え、比較した結果、前記格納する認証用データの付帯情報が新しいと判断した場合は、前記格納する認証用データを前記端末装置に送信するとしてもよい。

ここで、前記記録媒体が、認証用データ自身も記録するとしてもよい。

[0157] ここで、前記記録媒体の代わりに通信媒体を利用するとしてもよい。

また、本発明は、記録媒体を利用する端末装置である。前記端末装置は、複数の認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接

続して複数の認証用データを入手して前記格納部のデータを更新する。

[0158] ここで、前記複数の認証用データのうち少なくとも1つは、前記端末装置自身の有効性を読出装置に提示するための認証用データであり、さらに、前記認証用データのうち少なくとも1つは、前記読出装置の有効性を検証するための認証用データであるとしてもよい。

ここで、前記端末装置自身の有効性を前記読出装置に提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する送信部を備えるとしてもよい。

[0159] また、本発明は、記録媒体を利用する端末装置である。前記端末装置は、1つの認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、
比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して前記認証用データを入手して前記格納部のデータを更新し、前記認証用データは、前記端末装置自身の有効性を前記読出装置に提示するための認証用データであり、さらに、前記認証用データは、前記読出装置の有効性を検証するための認証用データも含む。

[0160] ここで、前記端末装置自身の有効性を前記読出装置に提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する送信部を備えるとしてもよい。

また、本発明は、記録媒体から付帯情報を読み出す読出装置である。前記読出装置は、認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部と、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して認証用データを入手して前記格納部のデータを更新して、さらに、前記認証用データから前記端末装置自身の有効性を前記読出装置に提示するための部分認証用データを抽出して送信する送信部と、前記端末装置から部分認証用データを受信する受信部と、前記受信した部分認証用データを検証する検証部を備える。

[0161] ここで、前記読出装置はさらに、認証用データの付帯情報を格納する格納部と、記

録媒体から読み出した付帯情報と前記格納する付帯情報を比較する比較部と、データを送信する送信部を備え、比較した結果、前記格納する付帯情報が新しいと判断した場合は、前記格納する付帯情報を前記端末装置に送信するとしてもよい。

ここで、前記読出装置はさらに、認証用データを格納する格納部と、記録媒体から読み出した付帯情報と前記格納する認証用データの付帯情報を比較する比較部と、データを送信する送信部を備え、比較した結果、前記格納する認証用データの付帯情報が新しいと判断した場合は、前記格納する認証用データを前記端末装置に送信するとしてもよい。

[0162] また、本発明は、認証用データの付帯情報を記録する記録媒体である。端末装置は、認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して認証用データを入手して前記格納部のデータを更新して、さらに、前記認証用データから前記端末装置自身の有効性を前記読出装置に提示するための部分認証用データを抽出して送信する送信部を備える。前記記録媒体は、前記端末装置により利用される。

[0163] また、本発明は、認証用データである。前記認証用データは、端末装置の有効性を示すデータと、読出装置の有効性を示すデータが一体化されていることを特徴とする。

ここで、前記認証用データは、前記端末装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できるとしてもよい。

[0164] ここで、前記認証用データは、前記読出装置の有効性を示すデータに対しては、その全体に対して検証用データが付与されるとしてもよい。

ここで、前記認証用データは、前記読出装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できるとしてもよい。

[0165] ここで、前記認証用データは、その全体に対して検証用データが付与されていると

してもよい。

また、本発明は、認証用データである。前記認証用データは、有効であることを示すデータ、無効であること示すデータ、有効である区間を示すデータ、無効である区間を示すデータが混在し、少なくとも2つ以上の組み合わせにより構成されることを特徴とする。

[0166] ここで、前記認証用データは、区間を示すデータの場合、区間であることを示すフラグが存在するとしてもよい。

ここで、前記認証用データは、端末装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できるとしてもよい。

[0167] ここで、前記認証用データは、前記読出装置の有効性を示すデータに対しては、その全体に対して検証用データが付与されるとしてもよい。

ここで、前記認証用データは、前記読出装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できるとしてもよい。

[0168] ここで、前記認証用データは、その全体に対して検証用データが付与されているとしてもよい。

本発明によれば、再生装置が、自身が有効であることを示すリストを更新する際に、通信相手の読出装置が有効か無効か判断するためのリストも合わせて更新することで、再生装置における読出装置に関するリストの更新を強制化させることができる。これは、再生装置が、自身が有効であることを示すリストを更新しない場合、読出装置からのコンテンツの供給がストップされることから、再生装置によるリストの更新は必須となり、その更新と合わせて読出装置のリストを更新することにより実現できる。

[0169] また、本発明によれば、再生装置が、自身の有効性を示すリストと、通信相手である読出装置の有効性を判断するためのリストを保持することから、これら2つのリストを1つにして、自身の有効性を示すリストの更新が、通信相手の有効性を判断するリストの更新と等価になるようにすることでリストの更新を強制化することができる。

(12)上記の実施の形態及び変形例において、リストD、リストH及び証明書識別子

リストは、各装置に割り当てられた公開鍵証明書の識別子を記録しており、これらの識別子は、無効化された公開鍵証明書又は有効な公開鍵証明書を示すとしているが、本発明は、このような構成には限定されない。

[0170] 前記各リストに代えて、有効な装置を識別する有効識別子を記録している有効装置リスト及び無効な装置を示す無効識別子を記録している無効装置リストが存在するとしてもよい。パーソナルコンピュータ及びドライブ装置は、これらの有効装置リスト及び無効装置リストに基づいて、自身の装置の有効性を証明し、相手の装置の無効性を判定する。パーソナルコンピュータは、上記の実施の形態と同様にして、有効装置リストを更新するか否かを、その版数の新旧により判定し、更新すると判定する場合に、最新版の有効装置リストを取得し、有効装置リストを最新版の有効装置リストに更新するとともに、最新版の無効装置リストを取得し、保持している無効装置リストを取得した最新版の無効装置リストに更新する。

[0171] また、次のように構成してもよい。前記各リストに代えて、有効な装置を識別する有効識別子を記録している有効装置リスト及び無効な記録媒体を示す無効識別子を記録している無効媒体リストが存在するとしてもよい。パーソナルコンピュータ及びドライブ装置は、これらの有効装置リスト及び無効媒体リストに基づいて、装置の有効性及び記録媒体の無効性を判定する。パーソナルコンピュータは、有効装置リストを更新するか否かを、その版数の新旧により判定し、更新すると判定する場合に、最新版の有効装置リストを取得し、有効装置リストを最新版の有効装置リストに更新するとともに、最新版の無効媒体リストを取得し、保持している無効媒体リストを取得した最新版の無効媒体リストに更新する。

[0172] また、次のように構成してもよい。前記各リストに代えて、有効な装置を識別する有効識別子を記録している有効装置リスト、無効な装置を識別する無効識別子を記録している無効装置リスト及び無効な記録媒体を示す無効識別子を記録している無効媒体リストが存在するとしてもよい。パーソナルコンピュータ及びドライブ装置は、これらの有効装置リスト、無効装置リスト及び無効媒体リストに基づいて、装置の有効性及び無効性並びに記録媒体の無効性を判定する。パーソナルコンピュータは、有効装置リストを更新するか否かを、その版数の新旧により判定し、更新すると判定する場

合に、最新版の有効装置リストを取得し、有効装置リストを最新版の有効装置リストに更新するとともに、最新版の無効装置リストを取得し、保持している無効装置リストを取得した最新版の無効装置リストに更新し、さらに、最新版の無効媒体リストを取得し、保持している無効媒体リストを取得した最新版の無効媒体リストに更新する。

[0173] また、次のように構成してもよい。前記各リストに代えて、有効な装置を識別する有効識別子を記録している有効装置リスト、無効な装置を識別する無効識別子を記録している無効装置リスト及び無効なデジタル著作物を示す無効識別子を記録している無効著作物リストが存在するとしてもよい。パーソナルコンピュータ及びドライブ装置は、これらの有効装置リスト、無効装置リスト及び無効著作物リストに基づいて、装置の有効性及び無効性並びにデジタル著作物の無効性を判定する。パーソナルコンピュータは、有効装置リストを更新するか否かを、その版数の新旧により判定し、更新すると判定する場合に、最新版の有効装置リストを取得し、有効装置リストを最新版の有効装置リストに更新するとともに、最新版の無効装置リストを取得し、保持している無効装置リストを取得した最新版の無効装置リストに更新し、さらに、最新版の無効著作物リストを取得し、保持している無効著作物リストを取得した最新版の無効著作物リストに更新する。

[0174] (13)本発明にかかる認証システムは、更新の強制力が働かない読出装置に対するリストの更新を、再生装置自身のリストの更新と同時に行う、あるいはリスト自身を一体化させることにより、効果的な認証を実現できるという効果を有し、公開鍵暗号を利用した認証システムにおいて有用である。

(14)本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

[0175] また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD−ROM、MO、DVD、DVD−ROM、DVD−RAM、BD(Blu−ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

[0176] また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

[0177] また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(15)上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

産業上の利用可能性

[0178] 本発明を構成する各装置、各方法、コンピュータプログラム、データ、コンピュータプログラム及びデータを記録している記録媒体は、認証を必要とするあらゆる産業において、経営的に、また継続的及び反復的に使用することができる。また、本発明を構成する各装置及び記録媒体は、電器機器製造産業において、経営的に、また継続的及び反復的に、製造し、販売することができる。

請求の範囲

[1] ブラックリストを用いて対象物が無効か否かを判定する判定装置であって、

対象物が無効か否かを示すブラックリスト及び自身が有効か否かを示すホワイトリストを保持する保持手段と、

前記ホワイトリストを更新するか否かを判定する判定手段と、

更新すると判定される場合に、最新のブラックリスト及び最新のホワイトリストを同時に取得する取得手段と、

取得した最新のブラックリスト及び最新のホワイトリストを前記保持手段に同時に上書きする更新手段と

を備えることを特徴とする判定装置。

[2] 前記対象物は、情報を記録するために用いられる記録媒体であり、

前記保持手段は、前記ブラックリストとして、前記記録媒体が無効か否かを示す媒体ブラックリストを保持しており、

前記取得手段は、前記最新のブラックリストとして、前記記録媒体が無効か否かを示す最新の媒体ブラックリストを取得し、

前記更新手段は、取得した前記媒体ブラックリストを前記保持手段に上書きすることを特徴とする請求項1に記載の判定装置。

[3] 前記対象物は、デジタル著作物であり、

前記保持手段は、前記ブラックリストとして、前記デジタル著作物が無効か否かを示す著作物ブラックリストを保持しており、

前記取得手段は、前記最新のブラックリストとして、前記デジタル著作物が無効か否かを示す最新の著作物ブラックリストを取得し、

前記更新手段は、取得した前記著作物ブラックリストを前記保持手段に上書きすることを特徴とする請求項1に記載の判定装置。

[4] 前記対象物は、情報取得装置であり、

前記保持手段は、前記ブラックリストとして、前記情報取得装置が無効か否かを示す装置ブラックリストを保持しており、

前記取得手段は、前記最新のブラックリストとして、前記情報取得装置が無効か否

かを示す最新の装置ブラックリストを取得し、

前記更新手段は、取得した前記装置ブラックリストを前記保持手段に上書きする

ことを特徴とする請求項1に記載の判定装置。

[5] 前記情報取得装置は、情報を記録するために用いられる記録媒体に対して情報を書き込み又は前記記録媒体から情報を読み出す媒体アクセス装置である

ことを特徴とする請求項4に記載の判定装置。

[6] 前記情報取得装置及び前記媒体アクセス装置は、一体の装置として構成される

ことを特徴とする請求項5に記載の判定装置。

[7] 前記情報取得装置は、デジタル放送により放送される情報を受信するデジタル放送受信装置である

ことを特徴とする請求項4に記載の判定装置。

[8] 前記判定手段は、前記ホワイトリストの世代を示す世代情報を用いて、更新の判定を行う

ことを特徴とする請求項1に記載の判定装置。

[9] 前記判定手段は

前記対象物から適用すべきホワイトリストの世代を示す第1世代情報を取得する第1取得部と、

前記保持手段に保持されている前記ホワイトリストの世代を示す第2世代情報を取得する第2取得部と、

取得した第1世代情報と取得した第2世代情報とが示す各世代の新旧を比較し、第1世代情報が示す世代が第2世代情報が示す世代より新しい場合に、前記ホワイトリストを更新すると判断する判断部とを含む

ことを特徴とする請求項8に記載の判定装置。

[10] 前記第1取得部は、前記第1世代情報として、適用すべきホワイトリストの世代を示す第1バージョン番号を取得し、

前記第2取得部は、前記第2世代情報として、前記保持手段に保持されている前記ホワイトリストの世代を示す第2バージョン番号を取得し、

判断部は、第1バージョン番号と第2バージョン番号とを比較する

ことを特徴とする請求項9に記載の判定装置。

[11] 前記ブラックリストには、無効な対象物を識別する無効識別子が含まれ、

前記判定装置は、さらに、

前記ブラックリストに含まれる無効識別子を用いて、前記対象物が無効か否かを判定する無効判定手段を含む

ことを特徴とする請求項1に記載の判定装置。

[12] 前記ホワイトリストと前記ブラックリストとは、一体として1個のリストから構成される

ことを特徴とする請求項1に記載の判定装置。

[13] 前記ホワイトリストは、有効な対象物を識別する有効識別子、又は有効な対象物を識別する識別子の範囲を示す有効範囲情報を含み、

前記ブラックリストは、無効な対象物を識別する無効識別子、又は無効な対象物を識別する識別子の範囲を示す無効範囲情報を含む

ことを特徴とする請求項1に記載の判定装置。

[14] ブラックリストを用いて対象物が無効か否かを判定する判定装置と前記対象物とから構成される認証システムであって、

前記判定装置は、

対象物が無効か否かを示すブラックリスト及び自身が有効か否かを示すホワイトリストを保持する保持手段と、

前記ホワイトリストを更新するか否かを判定する判定手段と、

更新すると判定される場合に、最新のブラックリスト及び最新のホワイトリストを同時に取得する取得手段と、

取得した最新のブラックリスト及び最新のホワイトリストを前記保持手段に同時に上書きする更新手段とを備えることを特徴とする認証システム。

[15] コンピュータ読み取り可能であり、対象物が有効か否かを示すホワイトリストであって、

有効な対象物を識別する有効識別子、又は有効な対象物を識別する識別子の範囲を示す有効範囲情報を含む

ことを特徴とするホワイトリスト。

[16] コンピュータ読み取り可能であり、対象物が無効か否かを示すブラックリストであって、

無効な対象物を識別する無効識別子、又は無効な対象物を識別する識別子の範囲を示す無効範囲情報を含む

ことを特徴とするブラックリスト。

[17] ブラックリストを用いて対象物が無効か否かを判定する判定装置で用いられる判定方法であって、

前記判定装置は、対象物が無効か否かを示すブラックリスト及び自身が有効か否かを示すホワイトリストを保持する保持手段を備えており、

前記判定方法は、

前記ホワイトリストを更新するか否かを判定する判定ステップと、

更新すると判定される場合に、最新のブラックリスト及び最新のホワイトリストを同時に取得する取得ステップと、

取得した最新のブラックリスト及び最新のホワイトリストを前記保持ステップに同時に上書きする更新ステップと

を含むことを特徴とする判定方法。

[18] ブラックリストを用いて対象物が無効か否かを判定する判定装置で用いられる判定用のコンピュータプログラムであって、

前記判定装置は、対象物が無効か否かを示すブラックリスト及び自身が有効か否かを示すホワイトリストを保持する保持手段を備えており、

前記コンピュータプログラムは、

前記ホワイトリストを更新するか否かを判定する判定ステップと、

更新すると判定される場合に、最新のブラックリスト及び最新のホワイトリストを同時に取得する取得ステップと、

取得した最新のブラックリスト及び最新のホワイトリストを前記保持ステップに同時に上書きする更新ステップと

を含むことを特徴とするコンピュータプログラム。

[19] 前記コンピュータプログラムは、コンピュータ読み取り可能な記録媒体に記録されて

いる

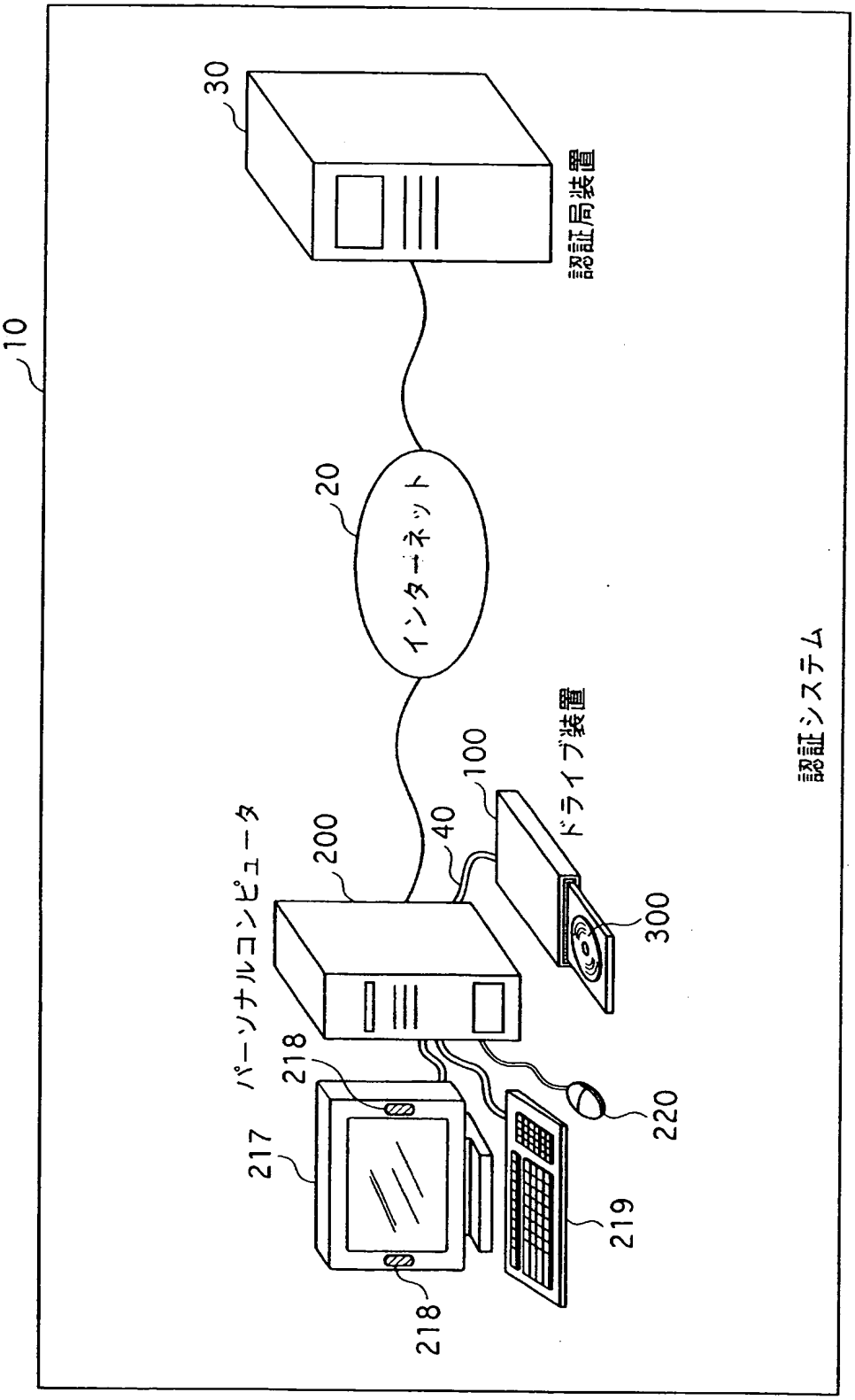
ことを特徴とする請求項18に記載のコンピュータプログラム。

[20] 前記コンピュータプログラムは、搬送波に乗せられて伝送される

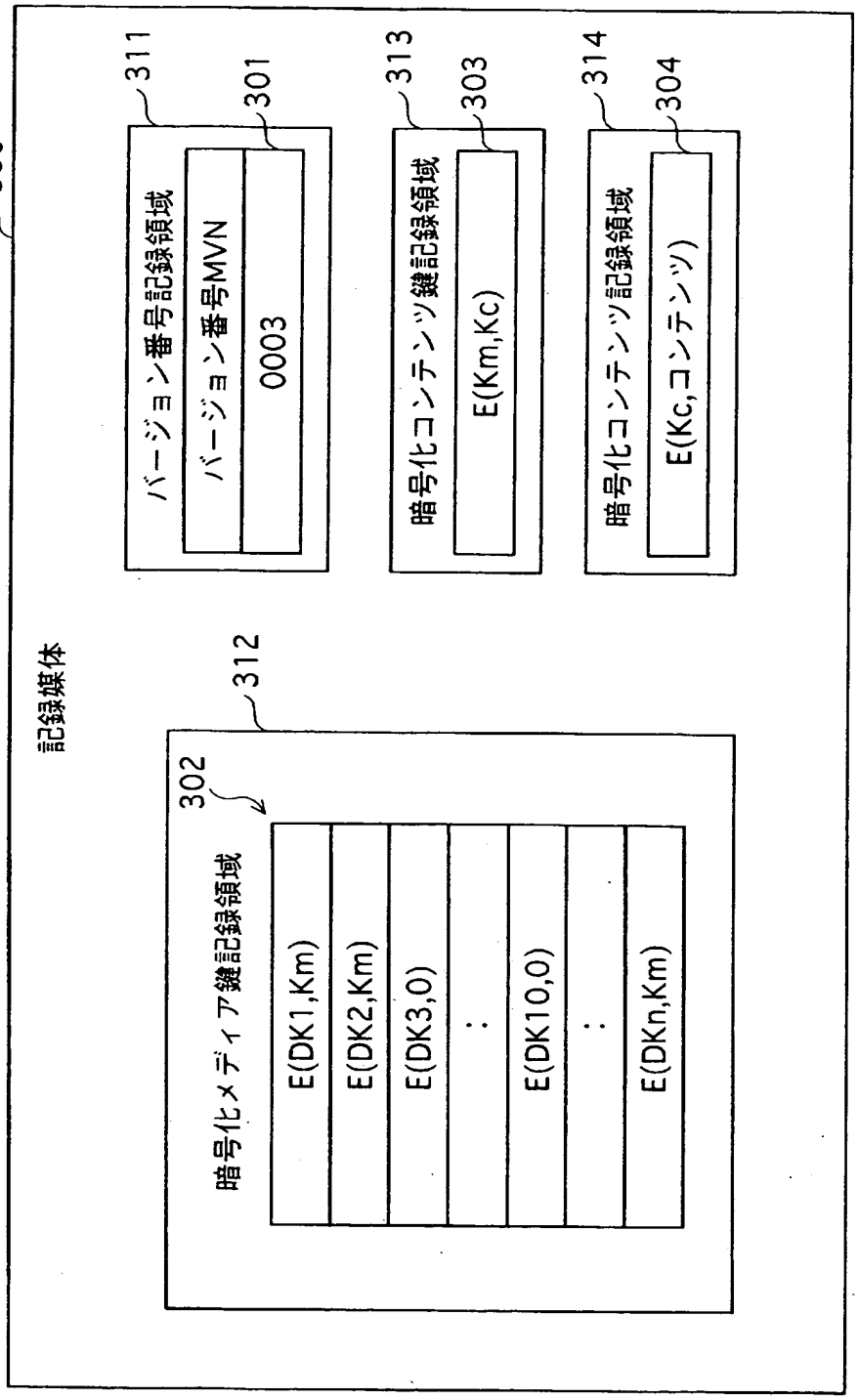
ことを特徴とする請求項18に記載のコンピュータプログラム。

WO 2005/052802 PCT/JP2004/017415

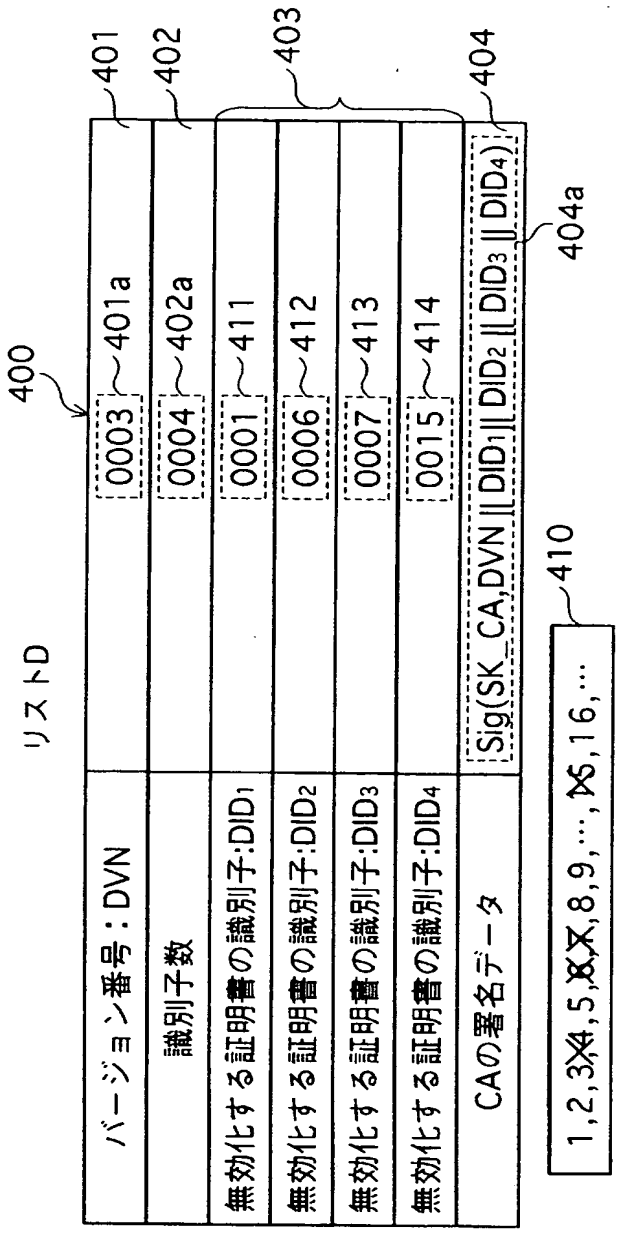
[図1]



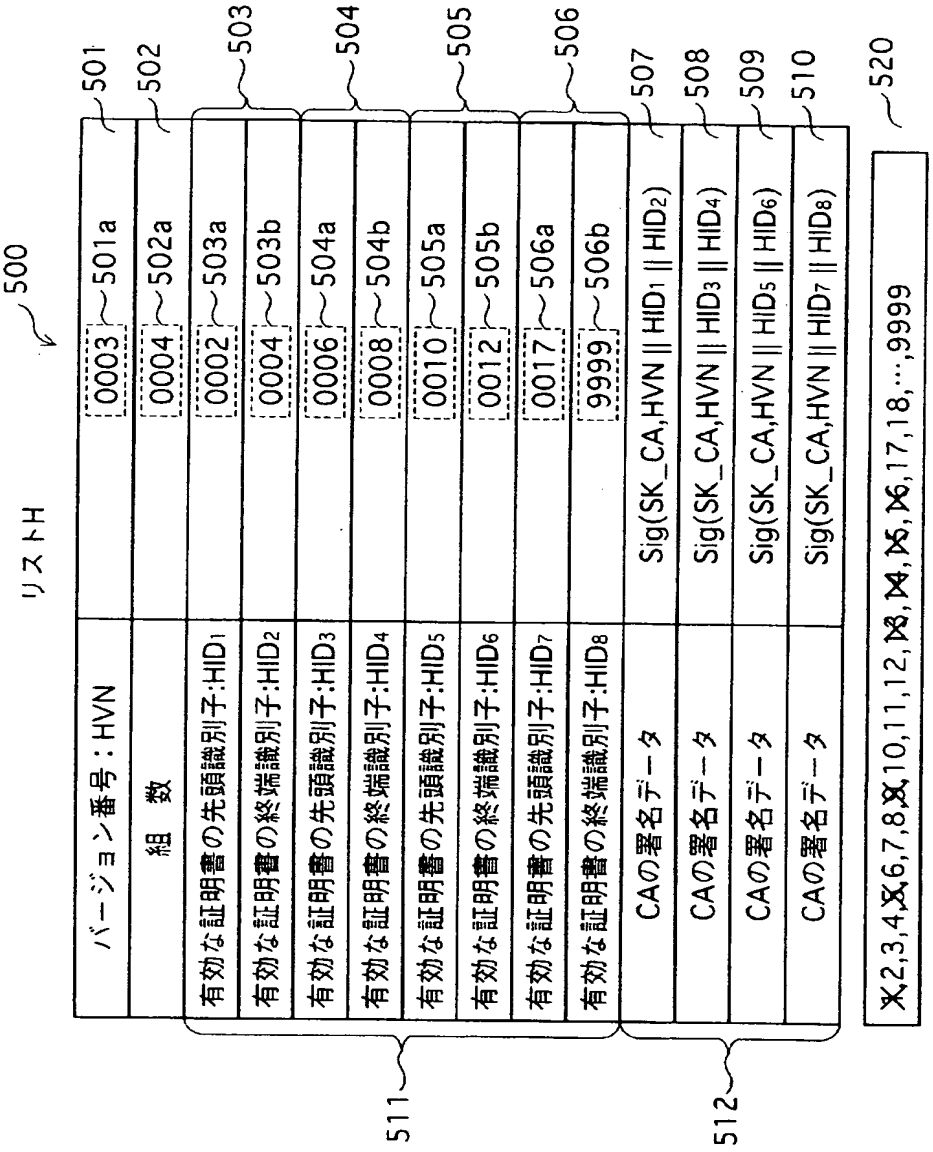
[図2]


300
記録媒体
311
バージョン番号記録領域
バージョン番号MVN
301
0003
313
暗号化コンテンツ鍵記録領域
303
E(Km,Kc)
314
暗号化コンテンツ記録領域
304
E(Kc,コンテンツ)
312
302
暗号化メディア鍵記録領域
E(DK1,Km)
E(DK2,Km)
E(DK3,0)
E(DK10,0)
E(DKn,Km)

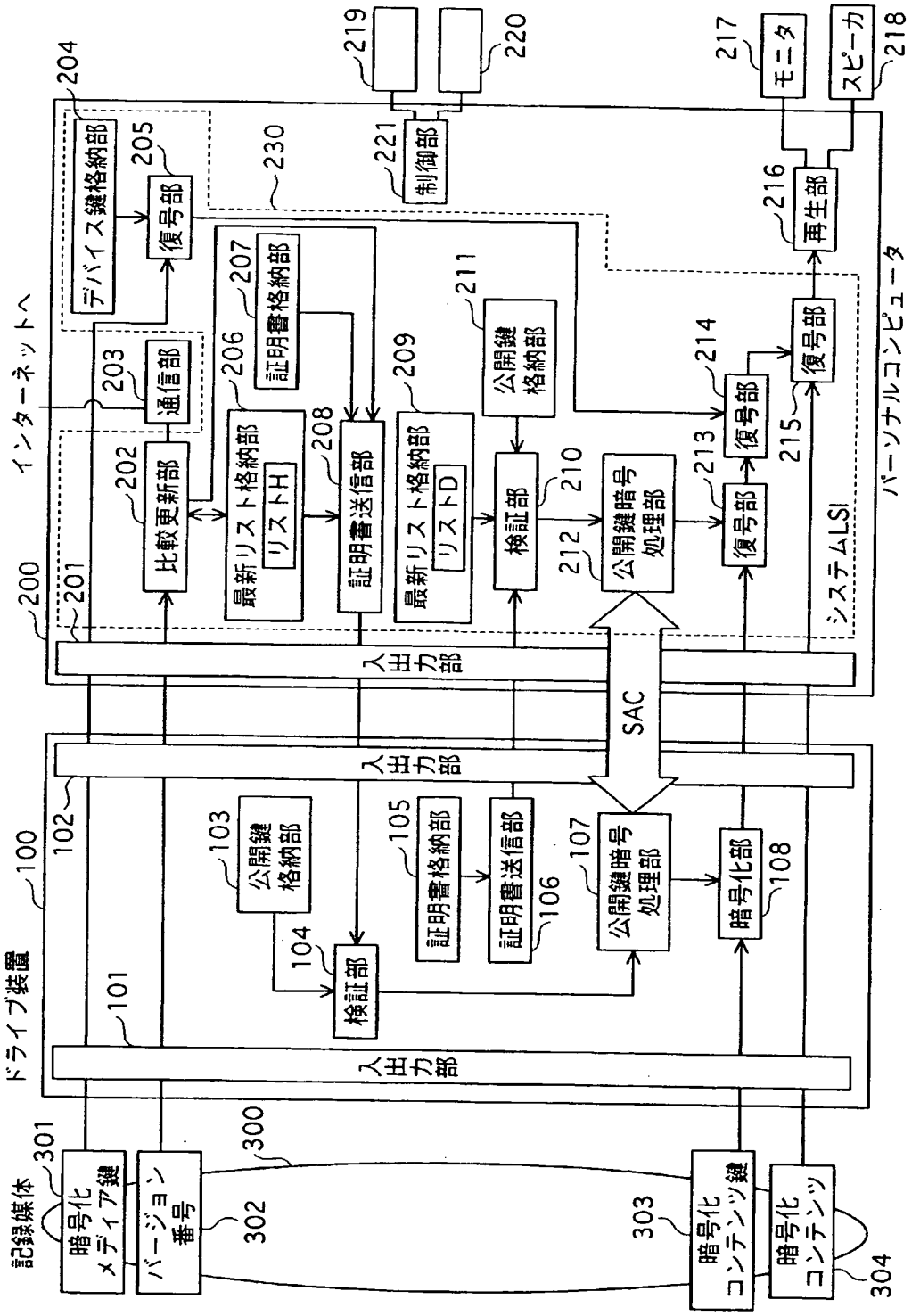
[図3]


400
リストD
401
402
403
404
404a
410
バージョン番号：DVN
識別子数
無効化する証明書の識別子:DID1
無効化する証明書の識別子:DID2
無効化する証明書の識別子:DID3
無効化する証明書の識別子:DID4
CAの署名データ
0003
0004
0001
0006
0007
0015
401a
402a
411
412
413
414
Sig(SK_CA,DVN || DID1 || DID2 || DID3 || DID4)
1,2,3,4,5,8,9,...,16,...

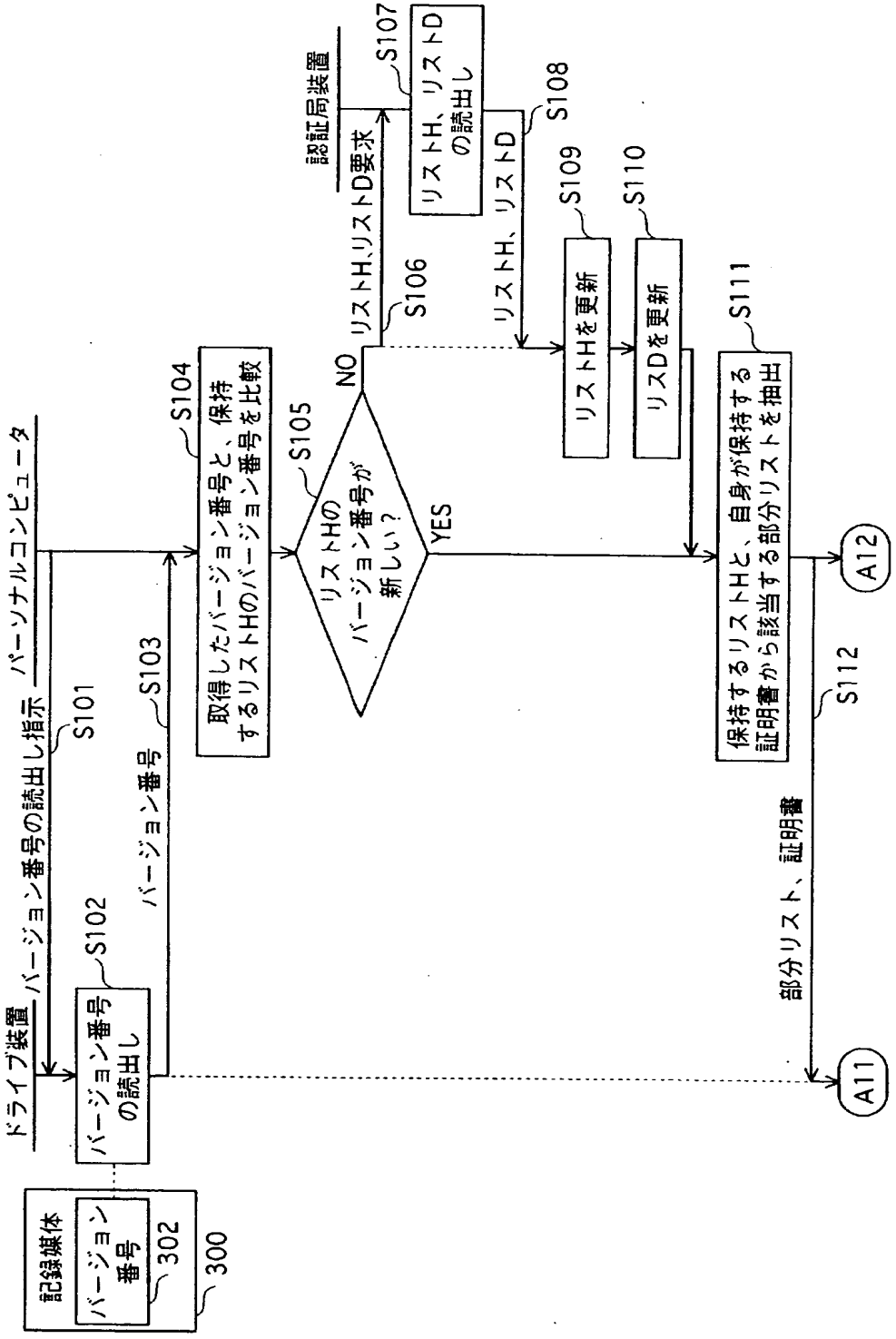
[図4]


500
リストH
501
502
503
504
505
506
507
508
509
510
520
511
512
バージョン番号：HVN
0003
501a
組　数
0004
502a
有効な証明書の先頭識別子:HID1
0002
503a
有効な証明書の終端識別子:HID2
0004
503b
有効な証明書の先頭識別子:HID3
0006
504a
有効な証明書の終端識別子:HID4
0008
504b
有効な証明書の先頭識別子:HID5
0010
505a
有効な証明書の終端識別子:HID6
0012
505b
有効な証明書の先頭識別子:HID7
0017
506a
有効な証明書の終端識別子:HID8
9999
506b
CAの署名データ
Sig(SK_CA,HVN || HID1 || HID2)
CAの署名データ
Sig(SK_CA,HVN || HID3 || HID4)
CAの署名データ
Sig(SK_CA,HVN || HID5 || HID6)
CAの署名データ
Sig(SK_CA,HVN || HID7 || HID8)
※2,3,4※6,7,8※10,11,12,※8,※4,※5,※6,17,18,…,9999

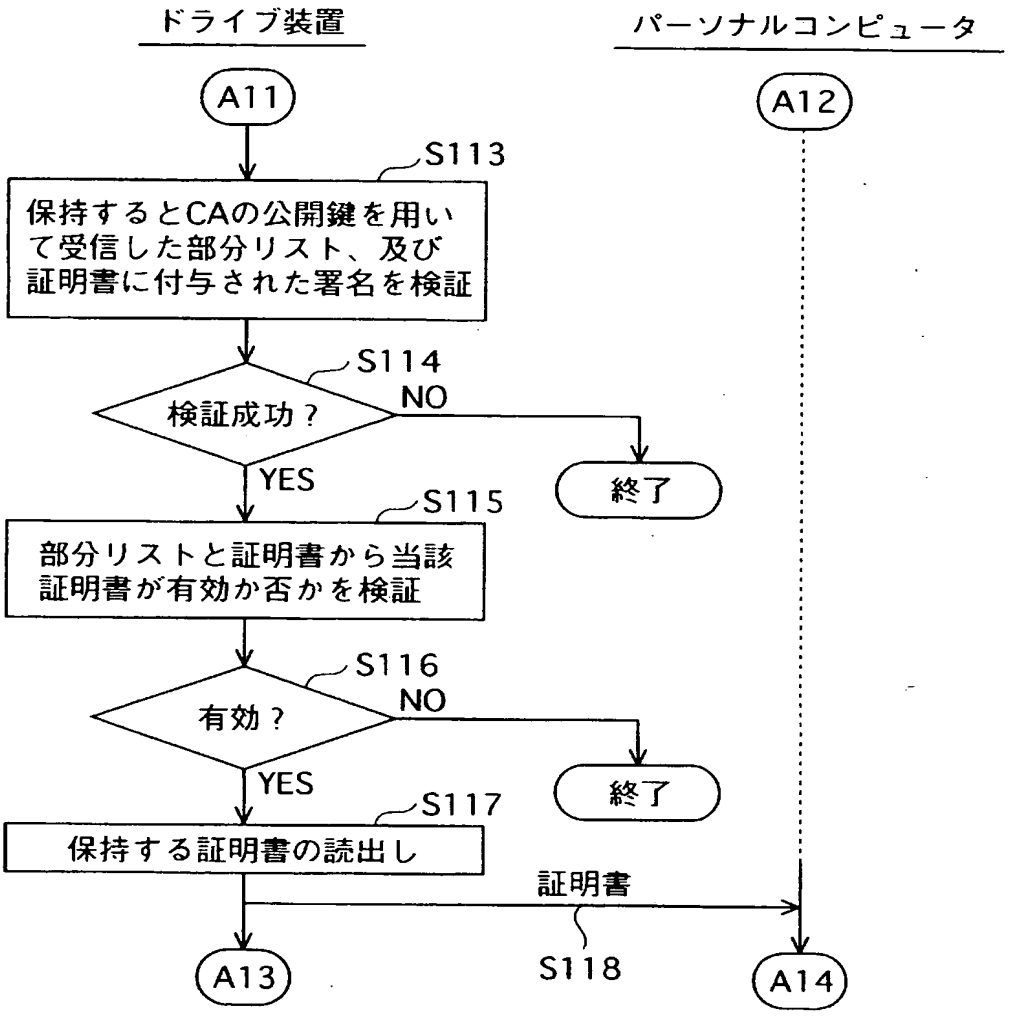
[図5]


ドライブ装置
記録媒体
暗号化メディア鍵
バージョン番号
暗号化コンテンツ鍵
暗号化コンテンツ
入出力部
公開鍵格納部
検証部
証明書格納部
証明書送信部
公開鍵暗号処理部
暗号化部
SAC
インターネットへ
通信部
比較更新部
最新リスト格納部
リストH
リストD
デバイス鍵格納部
復号部
制御部
再生部
モニタ
スピーカ
システムLSI
パーソナルコンピュータ

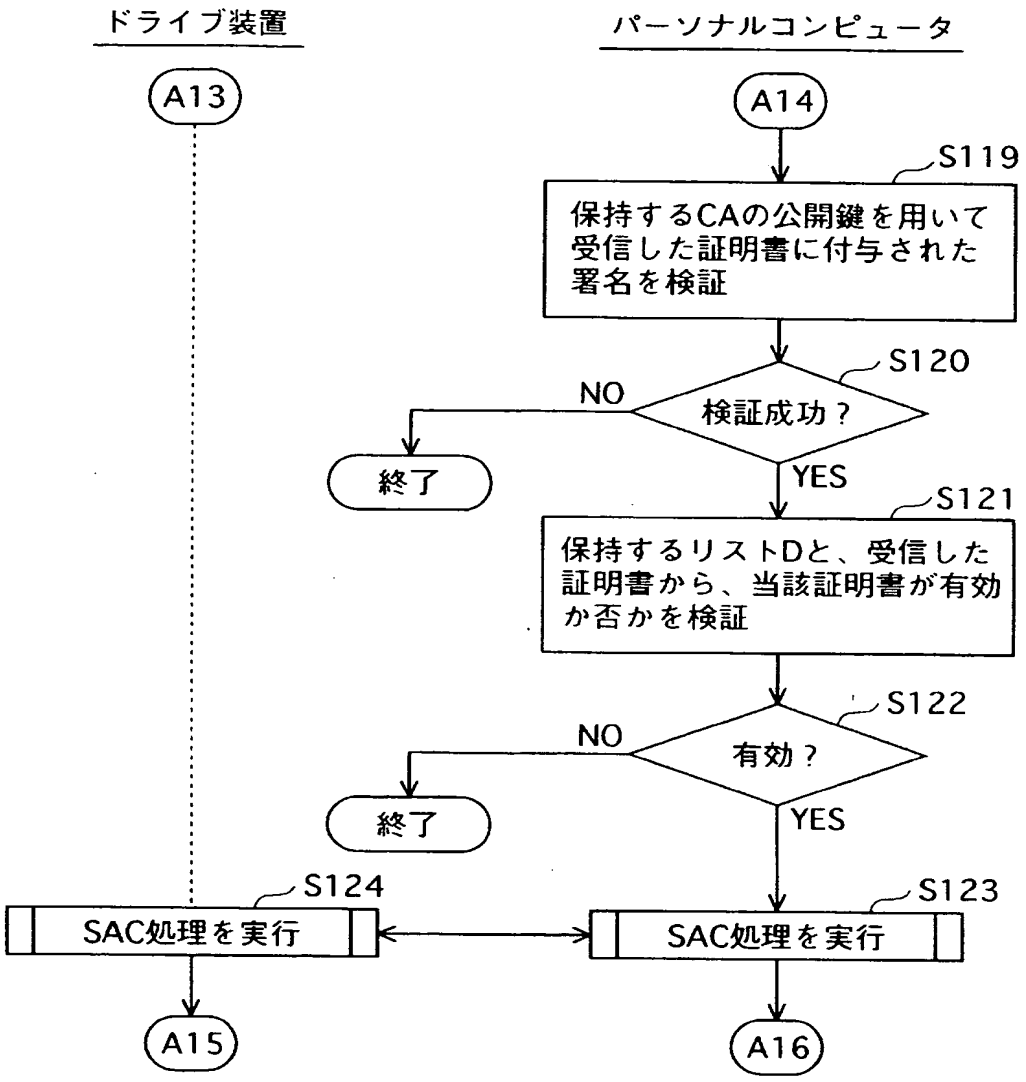
[図6]


記録媒体
バージョン番号
302
300
ドライブ装置
パーソナルコンピュータ
バージョン番号の読出し指示
S101
バージョン番号の読出し
S102
バージョン番号
S103
取得したバージョン番号と、保持するリストHのバージョン番号を比較
S104
リストHのバージョン番号が新しい？
S105
NO
YES
認証局装置
リストH,リストD要求
S106
リストH、リストDの読出し
S107
リストH、リストD
S108
リストHを更新
S109
リストDを更新
S110
保持するリストHと、自身が保持する証明書から該当する部分リストを抽出
S111
部分リスト、証明書
S112
A11
A12

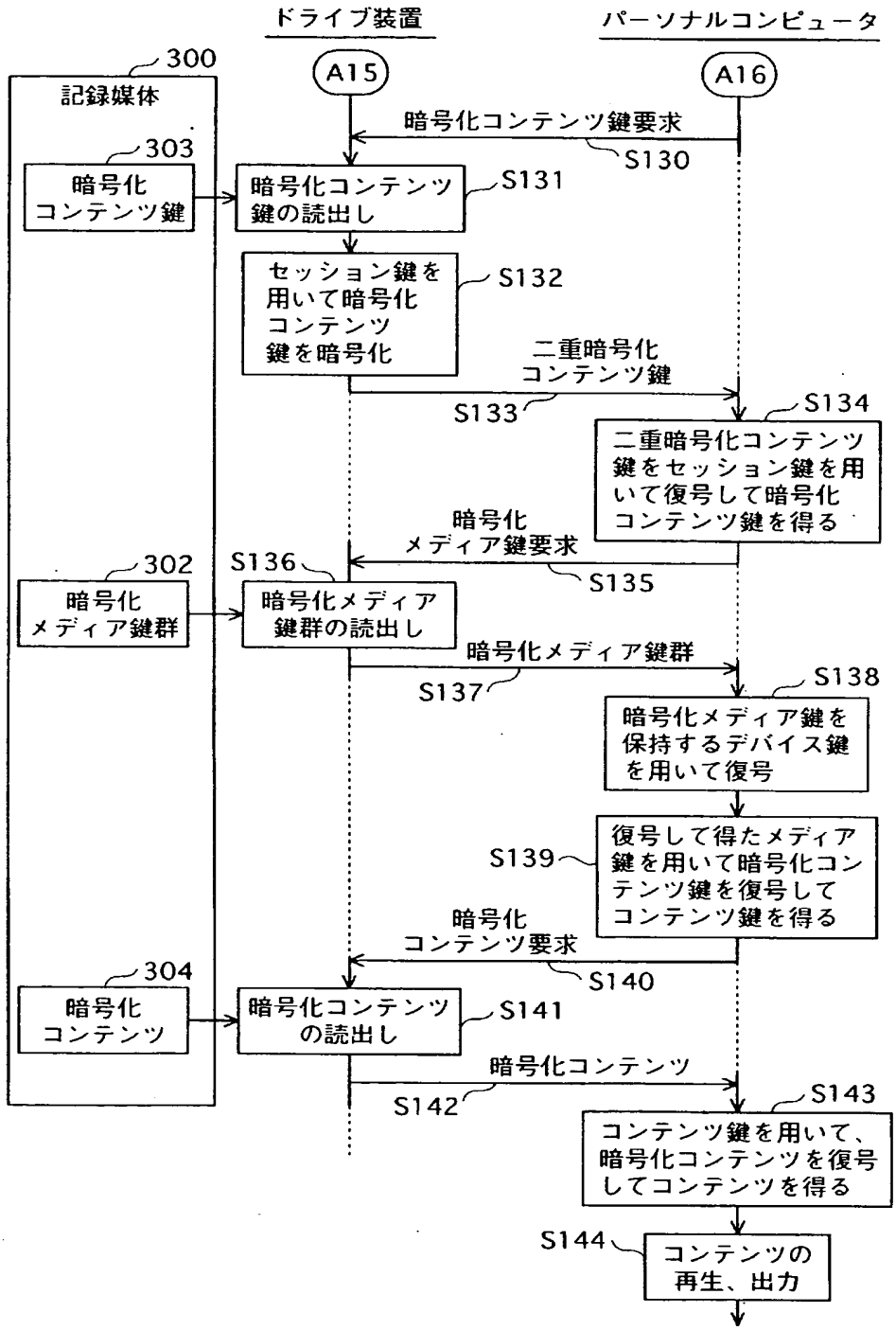
[図7]


ドライブ装置
パーソナルコンピュータ
A11
A12
S113
保持するとCAの公開鍵を用いて受信した部分リスト、及び証明書に付与された署名を検証
S114
検証成功？
NO
終了
YES
S115
部分リストと証明書から当該証明書が有効か否かを検証
S116
有効？
NO
終了
YES
S117
保持する証明書の読出し
証明書
S118
A13
A14

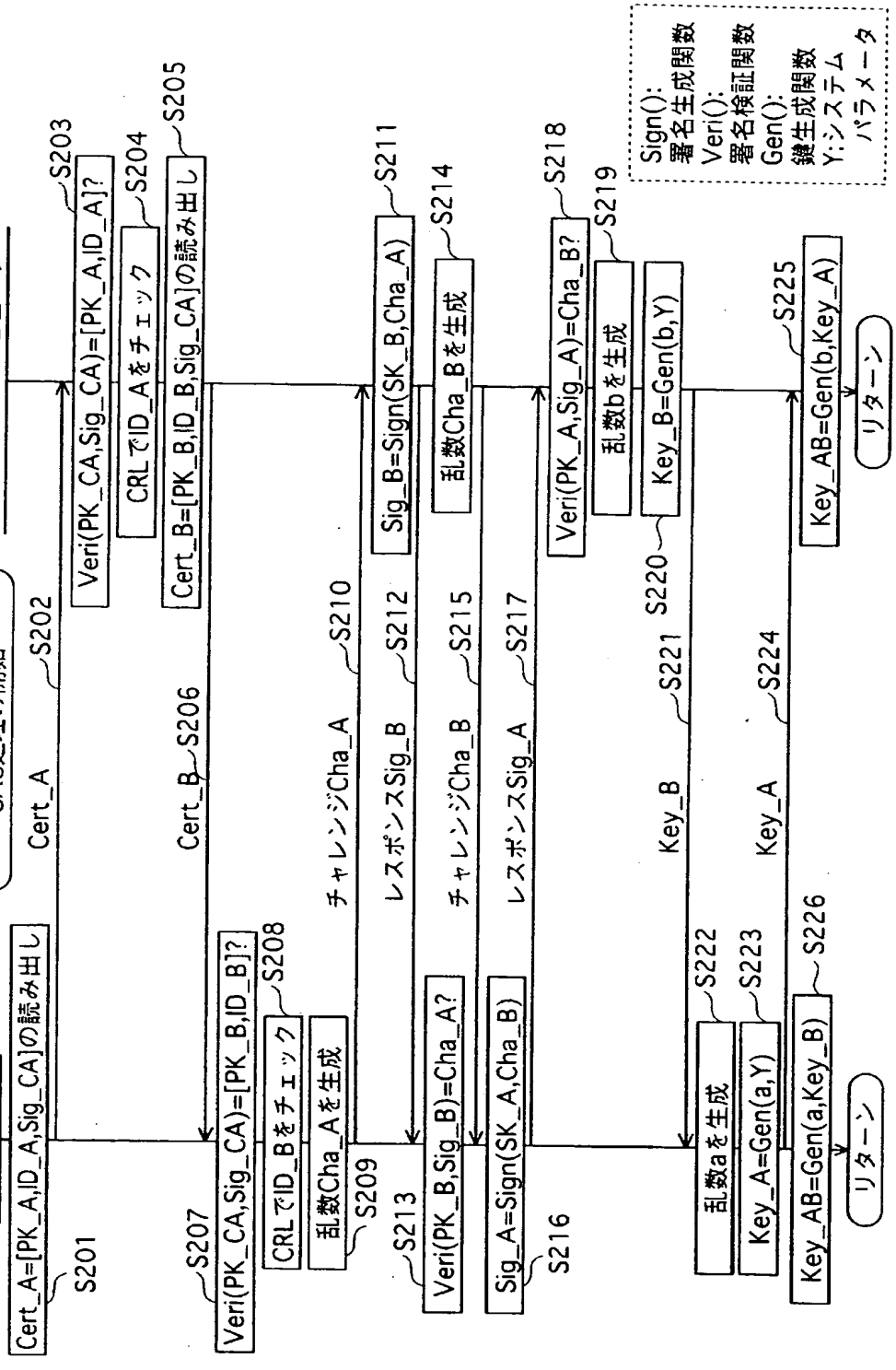
[図8]


ドライブ装置
パーソナルコンピュータ
A13
A14
S119
保持するCAの公開鍵を用いて受信した証明書に付与された署名を検証
S120
検証成功？
NO
YES
終了
S121
保持するリストDと、受信した証明書から、当該証明書が有効か否かを検証
S122
有効？
NO
YES
終了
S124
SAC処理を実行
S123
SAC処理を実行
A15
A16

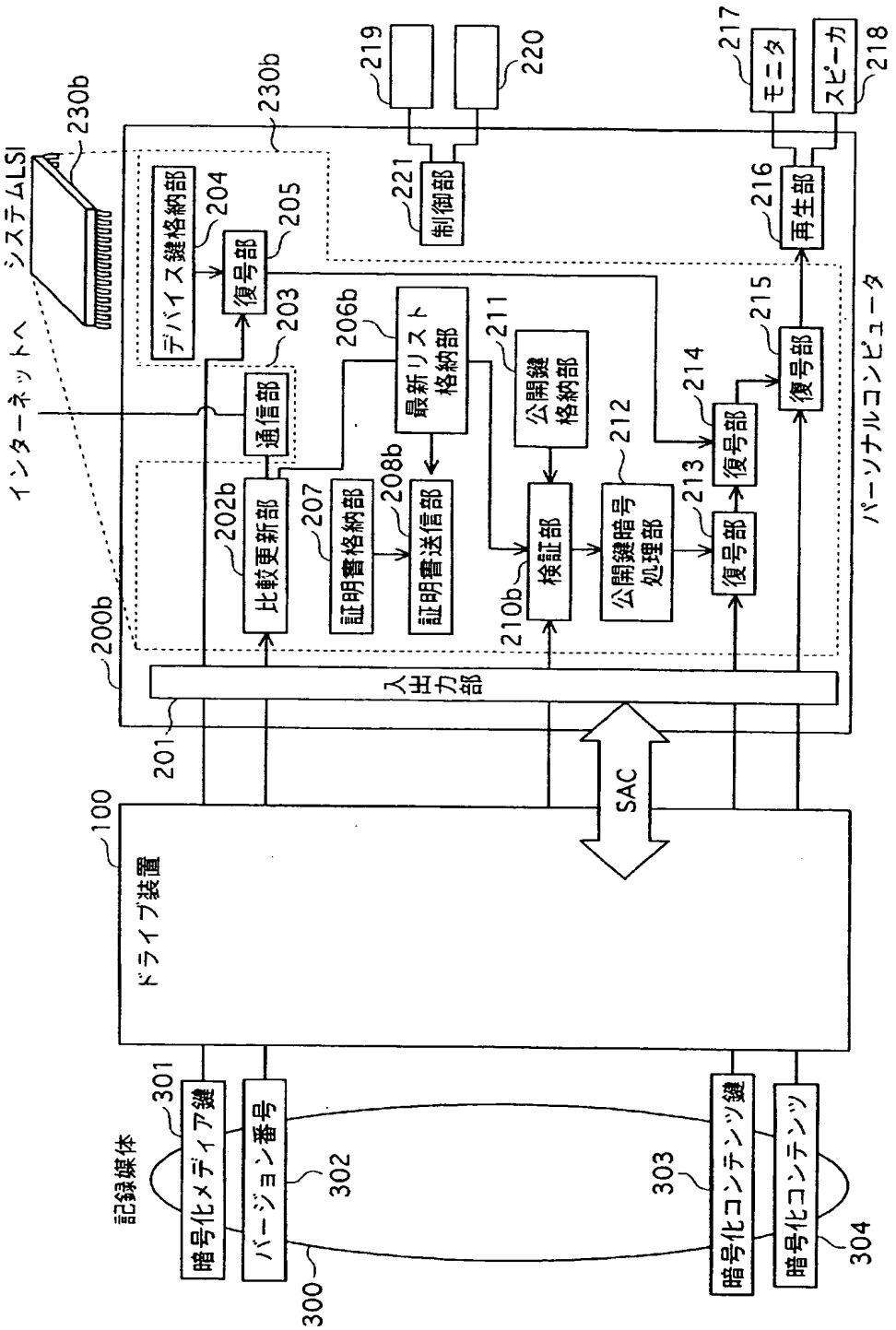
[図9]


ドライブ装置
パーソナルコンピュータ
300
記録媒体
A15
A16
暗号化コンテンツ鍵要求
S130
303
暗号化
コンテンツ鍵
暗号化コンテンツ
鍵の読出し
S131
セッション鍵を
用いて暗号化
コンテンツ
鍵を暗号化
S132
二重暗号化
コンテンツ鍵
S133
S134
二重暗号化コンテンツ
鍵をセッション鍵を用
いて復号して暗号化
コンテンツ鍵を得る
暗号化
メディア鍵要求
S135
S136
302
暗号化
メディア鍵群
暗号化メディア
鍵群の読出し
暗号化メディア鍵群
S137
S138
暗号化メディア鍵を
保持するデバイス鍵
を用いて復号
S139
復号して得たメディア
鍵を用いて暗号化コン
テンツ鍵を復号して
コンテンツ鍵を得る
暗号化
コンテンツ要求
S140
304
暗号化
コンテンツ
暗号化コンテンツ
の読出し
S141
暗号化コンテンツ
S142
S143
コンテンツ鍵を用いて、
暗号化コンテンツを復号
してコンテンツを得る
S144
コンテンツの
再生、出力

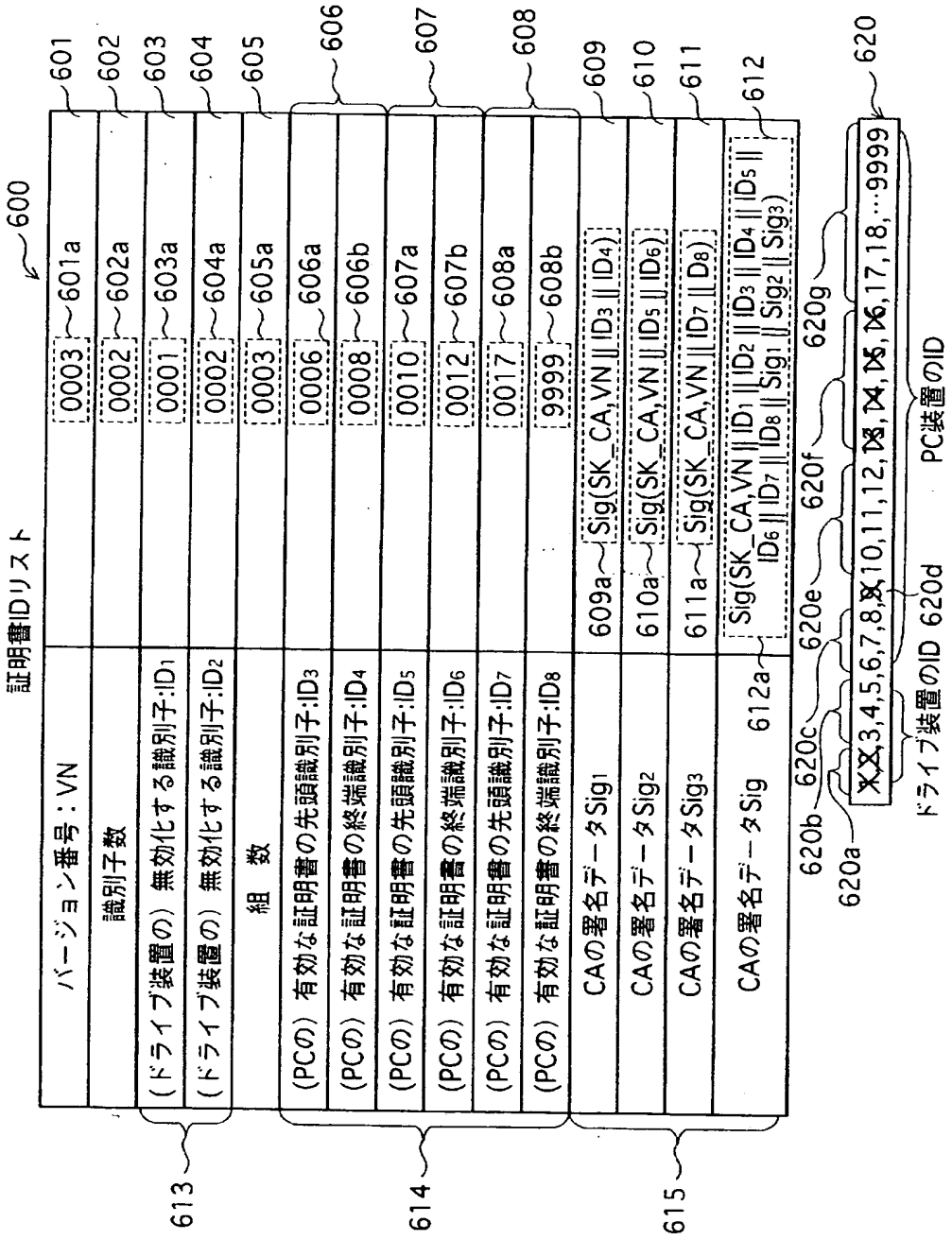
[図10]


ドライブ装置
パーソナルコンピュータ
SAC処理の開始
Cert_A=[PK_A,ID_A,Sig_CA]の読み出し
S201
Cert_A
S202
Veri(PK_CA,Sig_CA)=[PK_A,ID_A]?
S203
CRLでID_Aをチェック
S204
Cert_B=[PK_B,ID_B,Sig_CA]の読み出し
S205
Cert_B
S206
Veri(PK_CA,Sig_CA)=[PK_B,ID_B]?
S207
CRLでID_Bをチェック
S208
乱数Cha_Aを生成
S209
チャレンジCha_A
S210
Sig_B=Sign(SK_B,Cha_A)
S211
レスポンスSig_B
S212
Veri(PK_B,Sig_B)=Cha_A?
S213
乱数Cha_Bを生成
S214
チャレンジCha_B
S215
Sig_A=Sign(SK_A,Cha_B)
S216
レスポンスSig_A
S217
Veri(PK_A,Sig_A)=Cha_B?
S218
乱数bを生成
S219
Key_B=Gen(b,Y)
S220
Key_B
S221
乱数aを生成
S222
Key_A=Gen(a,Y)
S223
Key_A
S224
Key_AB=Gen(a,Key_B)
S226
リターン
Key_AB=Gen(b,Key_A)
S225
リターン
Sign():
署名生成関数
Veri():
署名検証関数
Gen():
鍵生成関数
Y:システム
パラメータ

[図11]

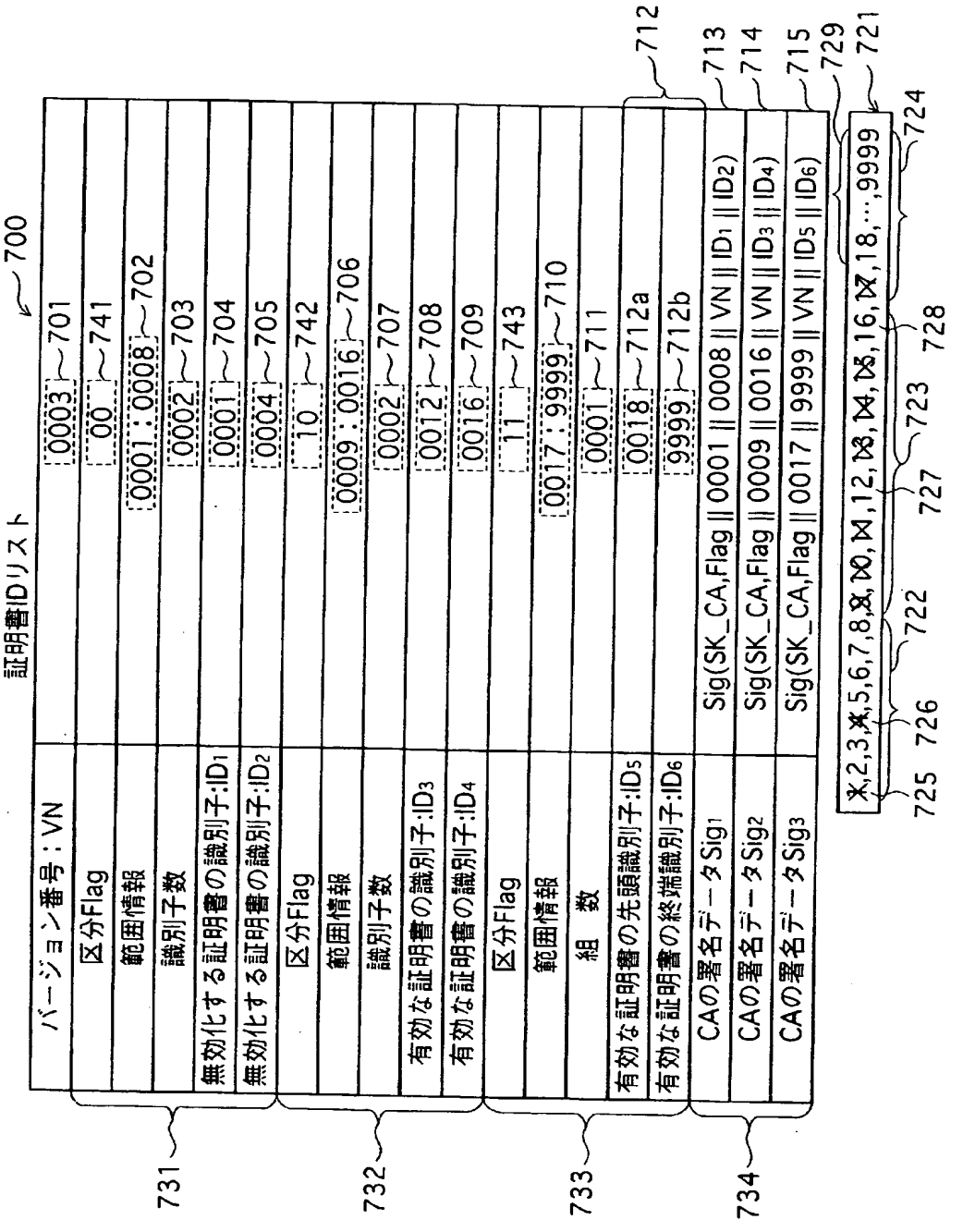

インターネットへ
システムLSI
230b
デバイス鍵格納部
204
復号部
205
203
通信部
202b
比較更新部
207
証明書格納部
208b
証明書送信部
206b
最新リスト格納部
211
公開鍵格納部
212
検証部
210b
公開鍵暗号処理部
213
復号部
214
復号部
215
復号部
216
再生部
217
モニタ
218
スピーカ
219
220
221
制御部
200b
入出力部
201
パーソナルコンピュータ
SAC
100
ドライブ装置
記録媒体
301
暗号化メディア鍵
バージョン番号
302
300
303
暗号化コンテンツ鍵
暗号化コンテンツ
304

[図12]


600
証明書IDリスト
601
602
603
604
605
606
607
608
609
610
611
612
バージョン番号：VN
識別子数
(ドライブ装置の) 無効化する識別子:ID1
(ドライブ装置の) 無効化する識別子:ID2
組 数
(PCの) 有効な証明書の先頭識別子:ID3
(PCの) 有効な証明書の終端識別子:ID4
(PCの) 有効な証明書の先頭識別子:ID5
(PCの) 有効な証明書の終端識別子:ID6
(PCの) 有効な証明書の先頭識別子:ID7
(PCの) 有効な証明書の終端識別子:ID8
CAの署名データSig1
CAの署名データSig2
CAの署名データSig3
CAの署名データSig
612a
0003
0002
0001
0002
0003
0006
0008
0010
0012
0017
9999
601a
602a
603a
604a
605a
606a
606b
607a
607b
608a
608b
609a
610a
611a
Sig(SK_CA,VN || ID3 || ID4)
Sig(SK_CA,VN || ID5 || ID6)
Sig(SK_CA,VN || ID7 || ID8)
Sig(SK_CA,VN || ID1 || ID2 || ID3 || ID4 || ID5 || ID6 || ID7 || ID8 || Sig1 || Sig2 || Sig3)
613
614
615
620
620a
620b
620c
620d
620e
620f
620g
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,…9999
ドライブ装置のID
PC装置のID

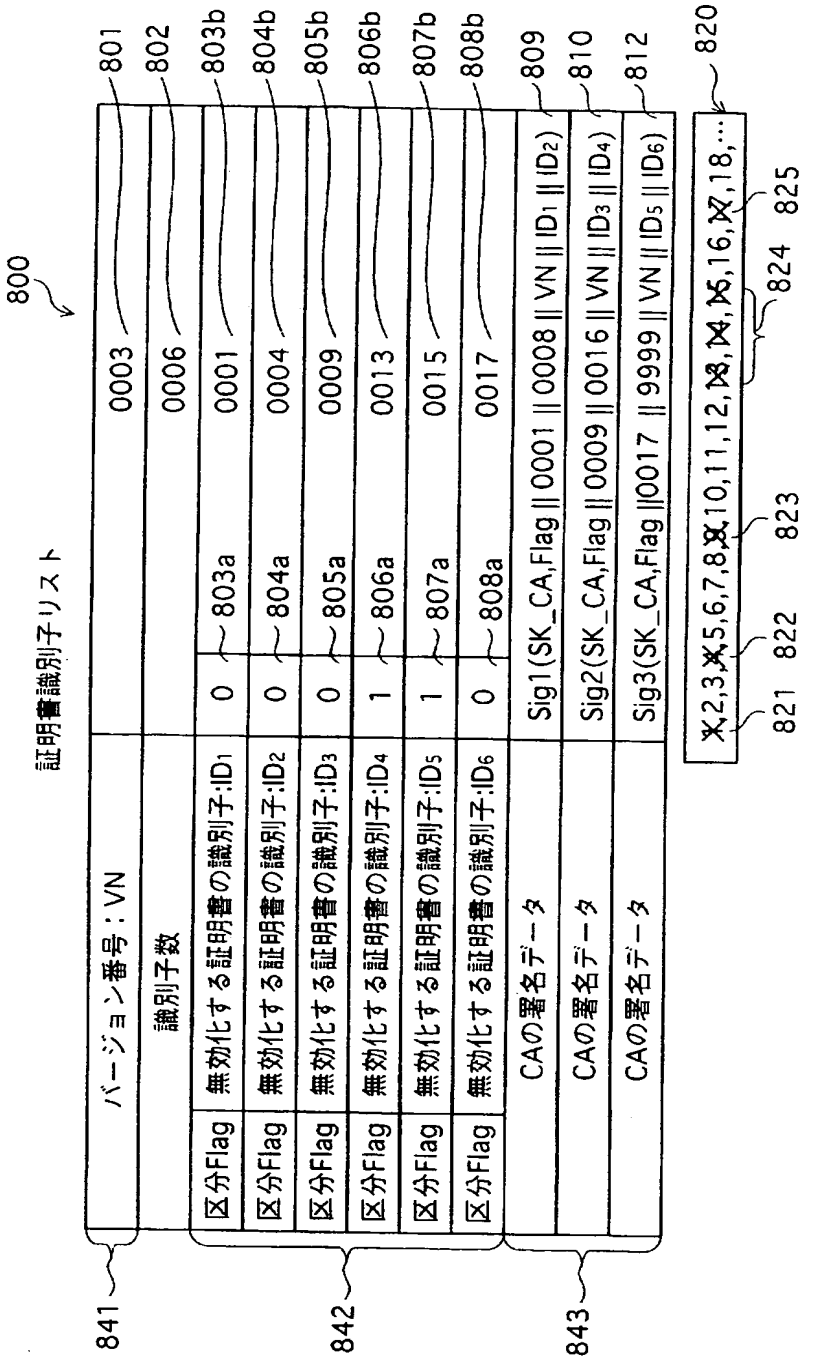
WO 2005/052802 PCT/JP2004/017415

[図13]



WO 2005/052802 PCT/JP2004/017415

[図14]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/017415

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/14, H04L9/00-9/38, G09C1/00-5/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho. 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002-0120847 A1 (Koninklijke Philips Electoronics N.V.), 29 August, 2002 (29.08.02), Full text; all drawings & WO 2002/067097 A2	1-14,17-20
A	JP 2002-135243 A (Sony Corp.), 10 May, 2002 (10.05.02), Full text; all drawings & WO 2002/033880 A1 & EP 1235380 A1 & US 2002/0184259 A1	1-14,17-20
A	US 5949877 A (Intel Corp.), 07 September, 1999 (07.09.99), Full text; all drawings & US 2002-0007452 A1	1-14,17-20

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 February, 2005 (16.02.05)	08 March, 2005 (08.03.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/017415

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 11-205305 A (Sony Corp.), 30 July, 1999 (30.07.99), Full text; all drawings & EP 0930556 A2	1-14,17-20
A	JP 2001-197054 A (Mitsubishi Denki Systemware Kabushiki Kaisha), 19 July, 2001 (19.07.01), Full text; all drawings (Family: none)	1-14,17-20
A	JP 2002-23627 A (Nippon Telegraph And Telephone Corp.), 23 January, 2002 (23.01.02), Full text; all drawings (Family: none)	1-14,17-20
A	JP 2003-115838 A (Matsushita Electric Industrial Co., Ltd.), 18 April, 2003 (18.04.03), Full text; all drawings & WO 2003/015344 A1 & EP 1414183 A1	1-14,17-20

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/017415

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [X] Claims Nos.: 15, 16
because they relate to subject matter not required to be searched by this Authority, namely:
Claim 8 relates to "a list" of predetermined information and falls in mere presentations of information which does nor require search by the International Search Authority under the provisions of PCT Article 17(2)(a)(i) and PCT Rule 39.1(v).

2. [ ] Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. [ ] Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. [ ] As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. [ ] As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

[ ] The additional search fees were accompanied by the applicant's protest.

[ ] No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号　PCT／JP2004／017415

A.　発明の属する分野の分類（国際特許分類（IPC））
Int.Cl⁷.　G06F12／14

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））
Int.Cl⁷.　G06F12／14，　H04L9／00－9／38，　G09C1／00－5／00

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　　1922－1996年
日本国公開実用新案公報　　1971－2005年
日本国実用新案登録公報　　1996－2005年
日本国登録実用新案公報　　1994－2005年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	US　2002－0120847　A1（Koninklijke Philips Electoronics N. V.）2002.08.29，全文，全図 & WO　2002／067097　A2	1－14，17－20
A	JP　2002－135243　A（ソニー株式会社）2002.05.10，全文，全図 & WO　2002／033880　A1 & EP　1235380　A1 & US　2002／0184259　A1	1－14，17－20

☒ C欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日
16.02.2005

国際調査報告の発送日　08.3.2005

国際調査機関の名称及びあて先
日本国特許庁（ISA／JP）
郵便番号100－8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）　5N　9290
相崎　裕恒

電話番号　03－3581－1101　内線　3585

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／０１７４１５

第Ⅱ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☒ 請求の範囲　１５，１６　は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、
請求の範囲８は、所定の情報の「リスト」であり、情報の単なる提示に該当し、PCT第17条(2)(a)(i)及びPCT規則39.1(v)の規定により、この国際調査機関が調査することを要しない対象に係るものである。

2．☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意
☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。